PRB - Audit & Eval.

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

SMALL BUSINESS/SELF-EMPLOYED DIVISION

RECEIVED
PROGRAM REVIEW BRANCH
NOV 13 2008

OCT 29 2008

RECEIVED
Employment Development Department
NOV 12 2008
DIRECTOR'S OFFICE

Patrick Henning
Director
Employment Development Department
800 Capitol Mall, MIC 83
617 N. Third Street
Sacramento, CA 95814

Dear Mr. Henning:

Enclosed for your review is the "Final" Safeguard Review Report (SRR), prepared as a result of our on-site review of the California Employment Development Department (EDD) conducted in January 2008. Our review was limited to the safeguards employed by your agency to protect the confidentiality of Federal tax information (FTI) disclosed to EDD pursuant to Internal Revenue Code Section 6103 (d), 6103(l)(10), 6103(m)(2) and Federal tax regulations 301.6103(p)(2)B-1 of the Internal Revenue Code.

Our "Final" report incorporates your agency's response to the "Interim" SRR. We have recently enhanced our method of monitoring the vulnerabilities identified in our safeguard reviews of agencies as well as the corresponding corrective actions advised, by use of our electronic database, Plan of Action & Milestones (POAM).

I want to thank-you for your continued cooperation in our efforts to protect Federal tax information. Overall, we believe that the California Employment Development Department is providing effective guidance to employees regarding the protection and confidentiality of federal tax return information.

Please extend a personal thanks to the agency staff for their cooperation and assistance during the safeguard review. We also appreciate your assistance in this matter and look forward to our continued positive relationship with your agency.

If you have general questions related to the Safeguard program, I can be reached at (202) 622-6807 or Janet.R.Miner@irs.gov. A member of your staff may contact Timothy P. Ladusky, of my staff, at (214) 413-5828 or Timothy.P.Ladusky@irs.gov

Sincerely,

Werner Hey

for Janet R. Miner
Acting Director, Office of Safeguards

Enclosure

Department of the Treasury
Internal Revenue Service

Safeguard Review Report

STATE OF CALIFORNIA

EMPLOYMENT DEVELOPMENT DEPARTMENT

October 2008

Final Report

State of California

Employment Development Department

INTRODUCTION — SECTION 1

Internal Revenue Code (IRC) §6103(d) authorizes the disclosure of Federal tax returns and return information (Federal tax information) to Federal, State and local agencies by the Internal Revenue Service (IRS). Return and return information with respect to taxes shall be open to inspection by, or disclosure to, any State agency, body or commission, or its legal representative, which is charged under the laws of such State with responsibility for the administration of State tax laws for the purpose of, and only to the extent necessary in, the administration of such laws, including any procedures with respect to locating any person who may be entitled to a refund.

As a condition for receiving Federal tax information (FTI), the California Employment Development Department (EDD) is required by Internal Revenue Code § 6103(p)(4) to establish and maintain, to the satisfaction of the Internal Revenue Service, certain safeguards designed to prevent unauthorized uses of the information and to protect the confidentiality of that information. In addition, IRC §6103(p)(8) provides that no return or return information shall be disclosed to any officer or employee of any State which requires a taxpayer to attach to, or include in, any State tax return a copy of any portion of his Federal return, or information reflected on such Federal return, unless such State adopts provisions of law which protect the confidentiality of the copy of the Federal return (or portion thereof) attached to, or the Federal return information reflected on, such State tax return.

IRC §6103(d) further allows for disclosures of FTI to officers and employees of the State audit agency for the purpose of, and only to the extent necessary in, making an audit of the State agency, body, or commission. This applies only to agency charged under the laws of the State with the responsibility for the administration of State tax laws.

Unlike other states that have a single department of revenue, California's state tax laws are administered by three separate state agencies. Employment Development Department (EDD) administers the state's employment taxes. California Franchise Tax Board (FTB) administers the California bank and corporation tax and the personal income tax laws. State Board of Equalization (BOE) administers the sales and use taxes and other special taxes and fees. While each agency has distinct responsibilities, their activities and administrative duties are similar and related to each other. For example, EDD relies on FTB for administration of the Excess state Disability Insurance Refund Program. EDD also collects and enforces the withholding for personal income taxes claimed on the state income tax returns processed by FTB. The close relationships between the agencies require frequent exchanges of confidential information and sharing of resources to be as efficient and effective as possible in fulfilling each agency's individual responsibilities.

The California State Legislature and the Governor have directed these three State tax agencies to work cooperatively together to maximize available resources to enforce existing state income, employment, sales and use and other tax programs. As a result, the three California state tax agencies have requested and received approval from the IRS for FTB to share Federal Tax Information (FTI) through the Fed/State Exchange Program (IRC 6103(d) with EDD and BOE. A letter from the IRS approved the data sharing on March 31, 2005 with a three year expiration date.

FTB maintains three automated systems to administer its personal income tax, business entity tax and non-filer compliance programs: Taxpayer Information system (TI), Business Entities Tax System (BETS), and the Integrated Non-filer Compliance (INC) System. These systems contain primarily state tax data, but also include FTI data elements obtained by FTB through the Fed/State Exchange Program. In conjunction with a strategic partnership between the three state agencies to improve the use tax information, a reciprocal agreement is in place that permits limited access by each agency to the other's automated systems. This access is authorized through a Governor's order, a well as legislatively mandated through statutes enacted in the California Revenue and Taxation Code and the Unemployment Insurance Code. The agencies' online access to these systems provides for greater efficiency and effectiveness in collection, audit and non-compliance activities for their respective tax programs.

CA EDD receives copies of IRS employment audit results (examination reports), Forms SS-8 (Employer-Employee Relationship Determinations) and FTI in response to ad hoc requests, per an exchange agreement with the IRS. CA EDD discontinued enrollment in the in the Fed/State Tape Exchange Program in 2001 due to its inability to read and process the information and the lack of programming resources to address that problem. Starting in 2008, EDD has re-enrolled in the

tape exchange program requesting only two IRS extracts, 1099-MISC 2006 and LEVY TY2007 by TIN. EDD uses the state and FTI data located on the FTB systems to enhance the agency's ability to obtain better address information (skip tracing), verify pertinent account information, and effectively resolve cases in a timely manner with collection and audit activities. The data provided through the online access considerably reduces the volume of manual requests for federal information that EDD employees would be required to submit to the IRS.

CA EDD has the Internet Field Office Compliance System (IFACS). IFACS is a workload management tool used to assign, track, transfer, or close collection activities relating to employer accounts. The system is used by EDD Tax Branch staff to match and review files for audit purposes.

Access to 1099-MISC information file has benefitted EDD's audit and collection programs immensely. In calendar year 2006, EDD used the information as one of its primary resources for audit leads to identify noncompliant employers, resulting in a total liability change of $6,070,117.00 and 750 audits. The 1099-MISC information enhanced EDD's collection program by enabling them to match (locate) data, identify revenue sources and aid in the determination of the collectability of an account, 27% of the account searched.

During the Safeguard Review, the following locations were visited:

EDD, 722 Capitol Mall, Sacramento, CA
DTS Cannery Campus, 1651 Alhambra Boulevard, Sacramento, CA
Investigations Bureau, 2411 Alhambra Boulevard, Sacramento, CA
Field Audit and Compliance Division/Underground Economy Office, 3321 Power Inn Road, Sacramento, CA

During the Safeguard review process, the team met with the following agency contacts:

- Bob Orr, Manager (Tax Administrator1)
- Sarah Smith, Student Assistant (TSD)
- Pam Harter, Senior Programmer Analyst (ASD)
- Linda Effron, Sr. Tac Compliance Representative
- Jennifer Fukunaga, Sr. Tax Compliance Representative
- Frances Soohoo, Tax Information Security Officer
- Roger Remedios, Sr. Management Auditor (A & ED)
- Cathy Dockter, Staff Management Auditor (A & ED)
- Trina Martinez, External Auditor Coordinator, External Audit Coordinator
- Theresa Robinson, Sr. Tax Compliance Representative

- Dale Morgan, Chief Information Security Officer
- John Cordani, BAH Safeguard consultant
- Erik Fay, Tax Administrator
- Ted Martell, ASG
- John Elorduy, Investigations Division
- Carol Frost, Asst. to Deputy Director
- Richard Curry, Division Chief, FACD
- Jerry Hicks
- Ted Martell, ASG
- John Elorduy, Investigations Division
- Carol Frost, Asst. to Deputy Director
- Richard Curry, Division Chief, FACD
- Jerry Hicks
- Tonia Lediju
- James Graston
- John Logan

Pursuant to IRC §6103(p)(4), Tom Batch, Disclosure Enforcement Specialist and John Cardoni of Booze-Allen Hamilton conducted a safeguard review of the CA EDD January 8-10, 2008. Bob Orr and Jennifer Fukunaga coordinated the review by ensuring that appropriate personnel were available for discussion and provided requested documentation for the review.

SCOPE SECTION 3

The purpose of a safeguard review is to evaluate the methods utilized to protect FTI from unauthorized use or disclosure. At the location, we reviewed the physical security features and procedures utilized by the CA EDD to process and protect the return information provided under IRC §6103(d) for use in the collection and enforcement of the withholding for personal income taxes claimed on the state income tax returns, employer audit activities and compliance issues for employer nonfilers. The review does not evaluate the administration of any EDD program beyond safeguarding policies and procedures, nor is it an evaluation of the collection process.

At each location, we discussed the procedures and protection used for processing, accessing and/or safeguarding FTI. Training and awareness activities were included in the discussions. During visits, employees and managers were interviewed: facilities and work areas toured and case files, operating manuals, training material and various documents were reviewed.

The recommendations from the 2004 Safeguard Review Report were reviewed. All recommendations had been appropriately addressed and or resolved.

A. MAINTAINING A SYSTEM OF STANDARDIZED RECORDS

Requirement: 26 USC §6103(p)(4)(A) requires that a permanent system of standardized records be kept which documents requests for, and disclosure of, returns or return information. Refer to Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, Section 3, pages 7 and 8.

A.1 FINDING: EDD maintains a permanent system of standardized records that documents requests for and disclosures of FTI.

DISCUSSION: Federal employment audit reports are mailed from the IRS to the EDD Chief, Audit Section. The Office manager or his designee opens the mail, the transmittal is signed and dated, and the employment audit reports are placed in a locked cabinet for storage. Only the Office Manager and Program Technician have keys. The responsible program technician is notified the employment audit reports have been received and are ready for processing. The program technician enters the date received, date on the IRS document, the federal employer identification number (EIN, name of the entity, state identification number, and area audit office (AAO) number into a computer database. Documents are batched by AAO and forwarded by mail to the appropriate office with a transmittal. Documents not forwarded are shredded. The disk on which information is recorded is stored in a locked container at all times when not in use. No information is kept on the computer hard drive.

The IRS Disclosure Office in Oakland, CA has responsibility for forwarding to CA EDD FORMS SS-8 received from the IRS Austin Compliance Center. The forms are routed through the EDD Underground Economy Office and transmitted to the Audit Section. The forms are logged indicating the account number, name, date assigned and the name of the supervisor to whom it is assigned. When the case is returned, the "date in" is added. The SS-8 is destroyed when the case is completed.

RECOMMENDATION: None, all requirements have been met.

A.2 FINDING: EDD meets the requirements for maintaining a permanent system of standardized records for magnetic tapes received from CA FTB.

DISCUSSION: The Tax Information Security Officer receives the tape from a CA FTB employee who hand delivers the magnetic tape. The tape is taken down to the Tax Accounting system and brought across the street to the "Solar" building where a work order is created by a Tax Accounting System (TAS) analyst. A courier transports the

magnetic tape to the IT Cannery site where it is loaded to the tape library. The tape run is scheduled and brings the information on to the mainframe. The courier returns the tape to the TAS office where it is picked up by a Tax Support Division employee. FTB is contacted, picks up and returns the tape to California Franchise Tax Board (CA FTB). Tapes are processed along mainframe. Data is not kept on mainframe. After 300 days, any backup tapes are scratched.

RECOMMENDATION: None, all requirements have been met.

A.3 **FINDING:** EDD has an adequate system for controlling FTI.

DISCUSSION: EDD has a permanent system of standardized records, which documents FTI that has been transferred to EDD examination reports and case files. In using FTI, EDD tax examiners may transcribe FTI into their examination reports. EDD tracks all their case files that have FTI. EDD employees are required to label and track commingled FTI by using the FACD online log from the date of the request to the date of destruction.

RECOMMENDATION: None, all requirements have been met.

B. MAINTAINING A SECURE PLACE FOR STORAGE OF TAX RETURNS AND RETURN INFORMATION

Requirement: 26 USC §6103(p)(4)(B) requires that a secure place or area be maintained where federal tax information is stored. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 4, pages 9 through 15.

B.1 FINDING: Federal tax information is properly stored and protected in the EDD headquarters building at 722 Capitol Mall, Sacramento, CA.

DISCUSSION: Entrances to the 2 main entrances are secure. Anyone without a card key must enter through the main entrance. Building security guards verify identification. A visitor's sticker badge is issued after information in a visitor's log book has been completed. All special visitors receive numbered badges. Visitors are directed to the building manager's office where a contact is called. The contact comes downstairs to the lobby and escorts the visitor to the area being visited. The visitor's badge is returned to the guard desk after completion of the visit. Card keys with photo identification are used by CA EDD employees are used for areas not open to the public. The entrance doors are locked after hours. The building is EDD owned and is not shared with any other state agencies. Janitorial services are performed during normal office hours. The Tax Information Security Officer receives FTI from the IRS Oakland Disclosure Office and the Fresno RAIVS Unit in response to individual requests from EDD employees. Until distributed to EDD employees, the FTI is maintained in a locked cabinet with a combination lock. Only authorized employees have the combination. Entrance to the Tax Information Security Officer's area is by card key only.

RECOMMENDATION: None, all requirements have been met.

B.2 FINDING: Federal tax information is properly stored and protected in the Field Audit and Compliance Office at 3321 Power Inn Road, Sacramento, CA.

DISCUSSION: Minimum Protection Standards (MPS) were met at the field office site. EDD shares the building with several other state agencies. Property management provides security guards on a 24-hour basis. The public does not have access to EDD space. All doors have combination locks. All EDD employees are aware of and instructed to abide by the *EDD Clean Desk Policy* and store confidential records in locked containers, file cabinets, and/or desk drawers during non-work hours. The

office manager or their designated backup is responsible for inspecting the area, locking all doors, and activating the alarm at the end of each workday. Closed audit files containing FTI are kept in the locked file room, in non-locking cabinets, commingled and labeled as FTI appropriately. Active working cases are kept at the employee's desk and are required to be locked in desk drawers during non-work hours. Pursuant to CA EDD FAC Notice No.04-01 (4-09-2004), all hard copy case files and associated diskettes must be clearly labeled to indicate that they contain FTI. The marking of the case file will take place when the FTI is received and placed in the file, and will be done by stamping or writing "contains FTI" on the outside of the case folder. The marking of the file diskette will be done the same way and will take place when case information has been saved.

RECOMMENDATION: None, all requirements have been met.

B.3 FINDING: Federal tax information is properly stored and protected in the Investigations Division office at 2411 Alhambra Blvd., Sacramento, CA.

DISCUSSION: Minimum Protection Standards (MPS) were met at the Investigations office site. The public does not have access to Investigations Division space. A visitors log is filled out at the reception area and visitors are escorted into the office. All doors have combination locks. All EDD Investigation employees are aware of and instructed to abide by the *EDD Clean Desk Policy* and store confidential records in locked containers, file cabinets, and/or desk drawers during non-work hours. The manager or his designated backup is responsible for inspecting the area, locking all doors, and activating the alarm at the end of each workday. Closed investigation files containing FTI are kept in the locked file room, in non-locking cabinets, commingled and labeled as FTI appropriately. Active working cases are kept at the employee's desk and are required to be locked in desk drawers during non-work hours. I reviewed 5 cases and although cases were marked FTI, the tax returns were 3rd party information supplied by the person being investigated, thus not FTI. This information is allowed in the case file as long as it is properly marked or stamped as being received from the person being investigated.

RECOMMENDATION: None, all requirements have been met.

B.4 FINDING: Federal tax information is properly stored and protected in the DTS Cannery Campus (Computing Center) at 1651 Alhambra Blvd., Sacramento, CA.

DISCUSSION: The DTS Cannery Campus processes information for various state agencies, in addition to CA EDD. The DTS Cannery maintains a browser based application, Intranet Field Audit Compliance System (IFACS) for CA EDD. The physical security for the entrance to and within the facility meets IRS standards. State of California employees occupy the facility 24 hours per day, 7 days a week. Contracted guard service is in place at the entrance at all times. Entrance to the facility is strictly controlled. All doors are monitored. Non-Data Center visitors who have a demonstrated need for frequent and regular Data Center access must go through a clearance process before being issued a Data Center cardkey. All other visitors are identified, authenticated and given a badge prior to admission through an automated access control visitor system. They must be escorted at all times by a Data Center employee, who meets them at the entrance, which is at the guard area. After admission to the work area, there is a holding area for additional verification prior to entry to the main work area. The entire building perimeter and all interior areas are continually monitored by the contracted guard service via closed circuit TV cameras. The guard service also conducts roving patrols and walkthroughs of the work areas and outside perimeter. There is an alarm system monitored 24 hours per day. Janitorial services are provided during the day.

Entrance to the computer room and tape library is further restricted via the cardkey access control system. The authorized employee's cardkey is coded to restrict access solely to areas within the Data Center where access is required. The computer room is not well inside the building – none of the walls face outside, nor are there any windows. Standard fire safety provisions for computer rooms are in place, including sprinklers and Halon for fire suppression.

RECOMMENDATION: None, all requirements have been met.

B.5 FINDING: All FTI transported is not maintained in a secure manner.

DISCUSSION: When receiving completed requests for information from the RAIVS unit, the Tax Information Security Office confirms the authorized user from their list. If there is no information sent by the RAIVS Unit, this information is sent to the requester in a regular envelope. A return copy of the information is also sent back to the RAIVS Unit in a regular envelope. If there is return

information received by the Tax Information Security Office, that information is sent to the requester in a double sealed envelope.

RECOMMENDATION: All FTI transported through the mail or courier/messenger service must be double sealed, that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designated official or delegate is authorized to open it. All shipments of FTI must be documented with a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged.

AGENCY RESPONSE: The Employment Development Department (EDD) is in compliance with Internal Revenue Service's (IRS) recommendation. The EDD's Administrative Circular No. 05-02B issued on May 3, 2005 provides packaging requirements for shipment of confidential information. It states that all packages containing FTI must be doubled-packed with a sealed, inner envelope/container and a sealed outer envelope or reinforced cardboard box. The Administrative Circular attachments also states logging and monitoring of packages containing. This policy remains in force.

IRS : Agency response accepted

B.6 FINDING: Under Federal tax regulations § 301.6103(p)(2)(B)-1, EDD receives FTI from CA FTB.

DISCUSSION: The Tax Information Security Officer receives the tape from a CA FTB employee who hand delivers the magnetic tape. The tape is taken down to the Tax Accounting system and brought across the street to the "Solar" building where a work order is created by a Tax Accounting System (TAS) analyst. A courier transports the magnetic tape to the IT Cannery site where it is loaded to the tape library. The tape run is scheduled and brings the information on to the mainframe. The courier returns the tape to the TAS office where it is picked up by a Tax Support Division employee. FTB is contacted, picks up and returns the tape to California Franchise Tax Board (CA FTB). Through out the process, the tape was not properly labeled as FTI and afforded the double sealed barrier of protection for FTI being transported as required by publication 1075.

RECOMMENDATION: None. EDD no longer receives magnetic tapes from CA FTB. CA FTB has notified CA EDD that they will no longer be supplying 1099-MISC information by magnetic tape. CA FTB will only supply the information by electronic transfer means should CA EDD wish to continue receiving it from them. EDD is now testing SDT and will secure 1099-MISC

and LEVY information directly through the Internal Revenue Service. However, should CA EDD receive any other FTI in the future from CA FTB, procedures must be in place to properly log, protect and identify the received FTI information.

AGENCY RESPONSE: If the EDD receives any other FTI in the future from the Franchise Tax Board, procedures will be in place to properly log, protect and identify the FTI information.

IRS: Agency response accepted

B.7 FINDING: There is no warning banner reflected on the computer screen before an employee signs on to the Intranet Field Audit Compliance System (IFACS) system banner reflected on the computer screen before an employee signs on to the IFACS system.

DISCUSSION: Based upon the review at the 3321 Power Inn Rd. office, there is no warning banner present on CA EDD's IFACS system.

RECOMMENDATION: As stipulated by OMB 1545-0962, a warning banner advising of safeguarding requirements should be displayed on the screen of any computer accessing a system that stores, processes, or transits FTI. Consult your legal counsel to confirm /modify the appropriate wording of the warning banner. The system must write the full banner to the screen and pause to permit the user to read the banner before allowing them to proceed. As approved by the Department of Justice:

Warning! BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM YOU ARE CONSENTING TO SYSYTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

OR:

This is a FTI specific warning banner:

WARNING

This system may contain government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject to the

individual to criminal and civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (The Taxpayer Browsing Protection Act) and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING

Another acceptable warning banner that includes the four elements discussed would be adequate: They are:

1. Government System
2. Authorized Usage
3. Monitoring
4. Subject to Federal/state criminal or civil penalties

CA EDD can use any of the above, or construct their own warning banner that includes the four items above.

AGENCY RESPONSE: The EDD is in compliance with IRS recommendation. The following warning banner was added to IFACS on June 20, 2008.

WARNING

By accessing and using this government computer system, you are consenting to system monitoring for law encfrcement and other purposes. Unauthorized use of, or access to, this computer system may subject you to criminal prosecution and penalties.

Prior to logging on IFACS, the above warning banner appears and pauses to permit the user to read the banner. Before allowing the user to log on the user must select OK

IRS: Agency response accepted:.

C. LIMITING ACCESS TO TAX DATA TO EMPOYEES OF THE AGENCY WHO HAVE A NEED-TO-KNOW AND WHO ARE AUTHORIZED TO HAVE ACCESS

Requirement: 26 USC §6103(p)(4)(C) requires that access to federal tax information be restricted to persons whose duties require access and to who disclosure may be made under provisions of law. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 5, pages 17 through 19.

C.1 FINDING: Access to FTI and areas containing FTI are restricted to those personnel with a "need to know" and who are authorized by law to have access to the FTI data.

DISCUSSION: Managers designate employees authorized to receive Federal tax information and ensure that those employees have a "need to know". When an employee EDD employee leaves the agency, the manager notifies the Tax Information Security Officer. EDD has written procedures for disclosing information to others than the data subject. Those procedures require a written consent to be presented to the Department within 30 days of the date the consent was signed. The only employees who have access to FTI requested on an individual basis are the Tax Information Security Officer and her assistant. When the FTI is received, it is logged and forwarded to the person who made the request. The Chief, Audit Section, Field Audit and Compliance Division, receives examination reports. Only a Tax Administrator and Program Technical have access to these reports before distribution to the appropriate field offices. Only designated employees my process these reports in field offices. Logs are maintained on who has control of these examination reports.

RECOMMENDATION: None, all requirements have been met.

C.2 FINDING: Contract cleaning crews and maintenance crews do not have access to FTI.

DISCUSSION: Based upon discussions held at several offices, it was determined that the maintenance and cleaning crews have access to the office areas during the day and possibly at night in some locations. However, these crews do not have access areas where FTI is stored without a BSCE employee being present. At DOIT, cleaning personnel are not allowed in the computer room unless there is at least one DOIT employee present and under no circumstances may any cleaning personnel be authorized to open an outside door to allow entry to an individual.

RECOMMENDATION: None, all requirements have been met.

C.3 **FINDING:** CA EDD restricts access to the FTI received from CA FTB.

DISCUSSION: CA EDD has approximately 400 IFACS Users. Approximately 150-200 IFACS Users have access to the screens that house the 1099-MISC data supplied by CA FTB. Auditing programs are in place that track the access to the IFACS system.

RECOMMENDATION: None, all requirements have been met.

D. PROVIDING OTHER SAFEGUARDS DETERMINED TO BE NECESSARY

Requirement: 26 USC §6103(p)(4)(D) requires that other safeguard measures be provided that the Secretary of the Treasury determines to be appropriate to protect confidentiality of federal tax return information. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 6, pages 25 and 26.

D.1 FINDING: EDD has computerized training and awareness programs for their employees. All affected employees have access and opportunity to review a computerized security awareness presentation on computers at their work stations.

DISCUSSION: EDD uses computer based training (CBT). Each employee is required to sign a Tax Branch Confidentiality statement annually (DE 7410). The EDD also has Information Practices Handbook which addresses confidentiality and disclosure concerns. Employees are advised of criminal penalties for unauthorized access as well as unauthorized access as well as unauthorized disclosure of information. The Tax Disclosure Office now requires written (e-mail) confirmation from each of the four Tax Branch Division Chiefs once all employees have completed the annual Tax Branch I *Confidential Information and Security Awareness* computer based training module. This module includes a UNAX section and specific references to the administrative and legal consequences for unauthorized access, use and disclosure of FTI.

RECOMMENDATION: None, all requirements have been met.

D.2 FINDING: CA EDD's awareness program has been expanded.

DISCUSSION: The Tax Disclosure Office has issued a series of periodic e-mails to CA EDD staff reminding them of the administrative and legal consequences for unauthorized access, use and disclosure of FTI.

RECOMMENDATION: None, all requirements have been met.

E. SUBMISSION OF REQUIRED SAFEGUARD REPORTS

Requirement: 26 USC §6103(p)(4)(e) requires that reports be furnished to the Secretary of the Treasury, which describes the procedures established and utilized to ensure the confidentiality of tax data received from the IRS. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 7.

E.1 **FINDING:** A Safeguard Procedure Report (SPR) was submitted as required and is on file.

DISCUSSION: EDD's SPR is dated January 1996. The new Publication 1075 outlines that an SPR is now due every six years or when significant changes occur in the agency. The Safeguards office will notify EDD when to file their updated SPR within the next year.

RECOMMENDATION: None, all requirements have been met. Upon notification by the Safeguards Office, a new SPR must be submitted with the Office of Safeguards.

E.2 **FINDING:** The Safeguard Activity Report (SAR) has been submitted as required and is on file.

DISCUSSION: The latest SAR is dated March 23, 2007, received on April 3, 2007 and accepted on May 4, 2007. Issues identified with shredding and 45 day contract notification was discussed and resolved with Julia Reasoner and Ike Grisby.

RECOMMENDATION: None, all requirements have been met.

F. DISPOSAL OF RETURNS AND RETURN INFORMATION UPON COMPLETION OF USE

Requirement: 26 USC §6103(p)(4)(f) requires agencies to return tax information to the IRS, make the information "undisclosable", or, in some instances, retain the information and safeguard it. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 8, pages 31 and 32

F.1 **FINDING:** Disposal of federal tax information at 3321 Power Inn Road meets appropriate standards.

DISCUSSION: The Field Audit and Compliance Division office has 2 sixty-four gallon Plastopan security bins. Review of 6 case files found no FTI present. All FTI is put into these shredding bins after use. Datashred Inc. contacts the office comes in and takes out the 2 shredding bins to their mobile shredding vehicle and shreds the material on-site. The office Tax Adminstrator witnesses the shredding from the shredding bins.

RECOMMENDATION: None, all requirements have been met.

F.2 **FINDING:** EDD/Datashred, Inc. contract #M660711 does not contain the appropriate safeguard language.

DISCUSSION: I reviewed the latest contract of Datashred Inc. (effective 5/1/2006 – 03/31/2008). The contract in Section II. E. Confidentiality of Data contains an outdated reference to Exhibit 5 in Publication 1075.

RECOMMENDATION: The current EDD/Datashred contract and all future contracts must include Publication 1075's, Exhibit 7 Contract Language For General Services which outlines the criminal and civil penalties for unlawful disclosure of Federal Tax Information and inspection of the offices by the IRS and the agency to verify the performance of work under this contract.

AGENCY RESPONSE: The EDD is in compliance with IRS recommendation. Publication 1075's Exhibit 7 is included in the current EDD/Datashed contract #M869121 (effective April1, 2008-March 31, 2009)

IRS: Agency response accepted

F.3 **FINDING:** EDD's Confidentiality Agreement that is attached to EDD/Datashred Inc. contract #M660711 and Department of Technology Services does not contain the appropriate safeguard language.

DISCUSSION: Agencies are encouraged to use specific safeguard language in their contractual agreements and confidentiality agreements to avoid ambivalence, ambiguity and advising all employees, contractors of the provisions of IRC §7213, 7213A and 7431.

RECOMMENDATION: All EDD current and future confidentiality agreements must include the provisions of IRC 7213, 7213A and 7431. Please refer to the language outlined in Publication 1075's Exhibit 10, IRC Sec. 7213 and 7213AUnauthorized Disclosure of Information and Exhibit 5, IRC 7431 Civil Damages for Unauthorized Disclosure of Returns and return information.

AGENCY RESPONSE: As of January 2008, all EDD confidentiality agreements involving FTI include the provisions of Internal Revenue Code 7213, 7213A, and 7431.

IRS: Agency response accepted.

G. NEED AND USE

Requirement: Policy Statement P-1-35 quotes that "Tax information provided by the IRS to State tax authorities will be restricted to the authorities' justified needs and uses of such information." Other agencies must use the information only for the purpose(s) authorized by statute.

G.1 **FINDING:** Federal tax data is used by the agency in accordance with the statute.

DISCUSSION: Disclosure of return information to the agency is prescribed by statute. Tax data disclosed to the California Employment Development Department under the provision of IRC §6103(p)(2) and IRC §6103(d) is used by the agency for use in audit leads for noncompliant employers by Field Audit and Compliance Division and by the Collection Division to locate delinquent taxpayers, identify revenue sources and aid in the determination of the collectability of an account.

EDD receives Form 1099-MISC information from the IRS through the Franchise Tax Board (FTB). FTB receives the tape of Form 1099-MISC as part of the Fed/State Data Exchange program. FTB adds to the tape the combined Federal/State Form 1099-MISC media filers and creates a California universe of form 1099-MISC filers. FTB provides the universe tape to the IRS, which upon receipt of a request from EDD provides the tape to the EDD.

In calendar year 2006, 750 audits were completed from the Form 1099-MISC data resulting in a total liability change of $6,070,117.00 with an average increase in liability of $8,093 per case. Since the Form 1099-MISC data became available in 2003, the Form 1099-MISC database is reviewed for most audit cases assigned. This gives the auditor the most complete picture of the employer before the first audit appointment. The audit program feels that access to this data enhances the productivity of every case, not just only the cases generated by the Form 1099-MISC data. The use of Form 1099–MISC information is critical to EDD's audit program and for promoting compliance.

In calendar year, 2006, EDD's Collection Division (CD) searched 922 accounts and 248 matching records were located using the Form 1099-MISC information. These results revealed an average success rate of 27% in locating data on delinquent accounts.

RECOMMENDATION: None, all requirements have been met.

G.2 **FINDING:** Unauthorized access or inspection of FTI must be reported.

DISCUSSION: If unauthorized use or access to FTI has been identified, either by review of the mainframe-access audit trail or by visual observation, the unauthorized disclosure must be reported to the Treasury Inspector General for Tax Administration (TIGTA).

RECOMMENDATION: Upon discovery of a possible improper inspection or disclosure of FTI by a Federal employee, a State employee, or any other person, the individual making the observation or receiving information should contact the office of the appropriate TIGTA.

Field Division	States Served by Field Division	Telephone Number
San Francisco	California, Hawaii	(510) 637-2558 Or 1-800-366-4484

The mailing address is:
Treasury Inspector General for Tax Administration
P. O. Box 589, Ben Franklin Station
Washington, DC 20044-0589

AGENCY RESPONSE: The EDD will adhere to IRS recommendation. Per California Civil Code 1798.29(b), upon discovery, the Tax Information Security Office will immediately notify the Treasury Inspector General for Tax Administration of any breach, improper inspection, or disclosure of the FTI.

IRS: Agency response accepted

H. COMPUTER SECURITY

Requirement: IRS Publication 1075 requires all systems that process Federal tax data to comply with the provisions of OMB Circular A-130 and Department of Treasury Directives. Computers, which process, store, or transmit Federal tax returns or return information shall meet the minimum security requirements and standards defined in the Publication 1075.

The California Employment Development Department (EDD) currently has one system that processes, stores and transmits Federal tax information (FTI).

1. IFAX: Intranet Field Audit Compliance System (IFAX) is used as a workload management tool to assign, track, transfer, or close collections activities relating to employer accounts. The system is used by EDD Tax Branch staff to match and review files for audit purposes. FTI is loaded on to the database server from the mainframe via FTP. Users access the application remotely through the Intranet via HTTPS. The servers are located at the state Data Center at 1651 Alhambra Blvd. Sacramento, CA 95816.

Note: EDD is not currently using Tumbleweed for transfer of FTI. Although the Tumbleweed infrastructure is in place and planned to come online in January, since FTI is not currently being processed by the Tumbleweed infrastructure it is excluded from the scope of this review.

1. MOT – Findings H.1 - H.15
2. UNIX (AIX) - Findings H.16-H.26
3. Windows 2003– Findings H.27 – H.43
4. RACF – Findings H.44 – H.48

Note: The MOT findings are reported for the first time in accordance with the Publication 1075 revised in October 2007.

H. COMPUTER SECURITY

Requirement: IRS Publication 1075 requires all systems that process Federal tax data to comply with the provisions of OMB Circular A-130 and Department of Treasury Directives. Computers, which process, store, or transmit Federal tax returns or return information shall meet the minimum security requirements and standards defined in the Publication 1075.

The California Employment Development Department (EDD) currently has one system that processes, stores and transmits Federal tax information (FTI).

1. IFAX: Intranet Field Audit Compliance System (IFAX) is used as a workload management tool to assign, track, transfer, or close collections activities relating to employer accounts. The system is used by EDD Tax Branch staff to match and review files for audit purposes. FTI is loaded on to the database server from the mainframe via FTP. Users access the application remotely through the Intranet via HTTPS. The servers are located at the state Data Center at 1651 Alhambra Blvd. Sacramento, CA 95816.

Note: EDD is not currently using Tumbleweed for transfer of FTI. Although the Tumbleweed infrastructure is in place and planned to come online in January, since FTI is not currently being processed by the Tumbleweed infrastructure it is excluded from the scope of this review.

1. MOT – Findings H.1 - H.15
2. UNIX (AIX) - Findings H.16-H.26
3. Windows 2003– Findings H.27 – H.43
4. RACF – Findings H.44 – H.48

Note: The MOT findings are reported for the first time in accordance with the Publication 1075 revised in October 2007.

MOT Findings (New)

The MOT findings resulted from the evaluation of agency specific management, operational, and technical controls focusing just on FTI. The findings listed in this section are not specific to a particular technology or a system but rather address agency wide management, operational, and technical issues related to FTI.

Management Controls – Risk Assessment

H.1 **FINDING**: According to the on-site evaluation performed risk assessment controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, four Risk Assessment controls were found to not be compliant with IRS Publication 1075 standards. EDD currently does not have formal risk assessment policies and procedures in place. Processes are not in place to track to perform vulnerability assessments. The four non-compliant controls under the Risk Assessment control family include:

1. Risk Assessment Policy and Procedures (RA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
2. Risk Threat Assessment (RA-3) EDD does not evaluate and analyze the current threats and vulnerabilities in its logical or physical environment.
3. Risk Assessment Update (RA-4): EDD does not update the risk assessment at a minimum of every three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security status of the system.
4. Vulnerability Scanning (RA-5): EDD does not scan for vulnerabilities in the information system on a periodic basis or when significant new vulnerabilities potentially affecting the system are identified and reported.

RISK: Strong risk assessment policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong risk assessment policy and procedures, EDD does not have a standardized approach to formally document and implement risk assessment policy and procedures.

Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to Agency operations, Agency assets, or individuals based on the operation of the information system. Without periodic updates, evaluation and analysis of these threats and vulnerabilities may become outdated; therefore, inadequate

levels of information security may be implemented on the system, potentially allowing unauthorized access.

Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred. Failure to conduct regular vulnerability scans of the information system may expose the system to preventable risks and costs.

RECOMMENDATION: EDD Management should:

1. RA-1: Risk Assessment Policy and Procedures:
    a. Risk assessment policy and procedures need to (i) exist; (ii) should be documented; (iii) and should be disseminated to appropriate elements within EDD.
    b. Risk assessment policy and procedures (i) should be periodically reviewed by responsible parties within the agency; and (ii) should be updated, when EDD review indicates updates are required.
    c. Risk assessment policy should address the purpose and scope of the control, and should address roles, responsibilities, management commitment, coordination among agency entities, and compliance.
2. RA-3: Complete periodic assessments to evaluate and analyze current threats and vulnerabilities to ensure the security surrounding the information system is adequate to protect the system from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.
3. RA-4: EDD management should update risk assessment documentation for the information system every three years, or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact system security, to ensure that the system controls are adequate to protect the system from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.
4. RA-5: Vulnerability scanning should be conducted on systems with FTI.
    a. EDD management should scan the information system for vulnerabilities quarterly or when significant new vulnerabilities that could potentially affect the system are identified and reported.
    b. EDD management should use scanning tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact.

AGENCY REPONSE: The EDD has a documented Risk Assessment Policy and a risk assessment plan to update and complete a comprehensive risk analysis cycle at least every two years as outlined in the Enterprise Risk Management

(ERM) Framework Policy, Executive Notice No. 08-01B and Risk Assessment Policy, Executive Notice No. 03-02B.

The DTS has various standards addressing risk assessment policy and procedures. The DTS has the following standards for this area. The DTS policies "3200 Threat Management Policy," "3308 Network Server Vulnerability Scan Procedure," and "3300 Vulnerability Management Policy" address these issues.

(See Attachments 2, 3, 5, 6, and 7)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Management Controls – Planning

H.2 **FINDING**: According to the on-site evaluation performed, security planning controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, no planning controls were found to be compliant with IRS Publication 1075 standards. EDD does not formalize and conduct security planning activities. Documentation of security planning activities was not presented. The six non-compliant controls under the Planning control family include:

1. Security Planning Policy and Procedures (PL-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
2. System Security Plan (PL-2): EDD does not develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization do not review and approve the plan.
3. System Security Plan Update (PL-3): EDD does not review the security plan for the information system at least annually and revise the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
4. Rules of Behavior (PL-4): EDD does not establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization does not receive signed acknowledgement from users indicating that they have read, understand, and agree to abide by the Rules of Behavior, before authorizing access to the information system and its resident information.
5. Privacy Impact Assessment Control (PL-5): EDD does not conduct a privacy impact assessment on the information system in accordance with OMB policy.

6. Security-Related Activity Planning (PL-6): EDD does not currently plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on Agency operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

RISK: Strong security planning policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong security planning policy and procedures, the Agency does not have a standardized approach to formally document and implement security planning policy and procedures.

RECOMMENDATION: EDD Management should:

1. PL-1: Security Planning Policy and Procedures:
    a. Security planning policy and procedures (i) exist, for each control; (ii) should be documented; (iii) and should be disseminated to appropriate elements within EDD.
    b. Security planning policy and procedures (i) should be periodically reviewed by responsible parties within EDD; and (ii) are updated, when EDD review indicates updates are required.
    c. Security planning policy should address the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.
2. PL-2: System Security Plan: Develop a security plan, in accordance with NIST SP 800-18 methodology, that provides an overview of the information system and a description of the security controls planned or in place for meeting the IRS Publication 1075 security requirements. Designated agency management officials should review and approve the security plan. The review of the security plan should contain acknowledgement and acceptance from designated agency officials, i.e. (Information Security Officer, System Owner, and Service Provider).
3. PL-3: System Security Plan Update: The system security plan should be reviewed annually, by EDD management. During reviews major changes to EDD information systems and problems with security plan implementation and security control enhancements should be considered for updates to the security plan.
4. PL-4: Rules of Behavior: EDD management shall establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. EDD management should receive signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.
5. PL-5 Privacy Impact Assessment: EDD management should conduct a privacy impact assessment on the information system in accordance with OMB policy.

6. PL-6 Security-Related Activity Planning: EDD management should plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on Agency operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

AGENCY REPONSE: The EDD is in compliance with PL-1 through PL-6. The EDD Information Security Policy protects EDD information, communications, networks, systems, applications, equipment, facilities, and other information assets and sets the information security standards as summarized below:

1. Information Security Policy
2. Organization Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Automated Systems Development and Maintenance
9. Business Continuity Planning Management
10. Compliance

The EDD is in compliance with IRS' recommendation. The EDD has a mandatory computerized security awareness training program for employees which must be completed on an annual basis. The Security Awareness Training and Education is managed by EDD's Information Security Office (ISO). Upon completion of this training, each employee is required to sign a Confidentiality Statement (DE 7410) which is filed in their personnel file.

(See Attachments 8, 9, and 10)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Management Controls – System & Services Acquisition

H.3 FINDING: System & Services Acquisition controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, ten System & Services Acquisition controls were found to not be compliant with IRS Publication 1075 standards. The ten non-compliant controls under the System & Services Acquisition control family include:

1. System and Services Acquisition Policy and Procedures (SA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented

procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

2. Allocation of Resources (SA-2): EDD does not determine, document, and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system.
3. Life Cycle Support (SA-3): EDD does not manage the information system using a system development life cycle methodology that includes information security considerations.
4. Acquisitions (SA-4): EDD does not include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
5. Information System Documentation (SA-5): EDD does not obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.
6. Software Usage Restrictions (SA-6): EDD does not comply with software usage restrictions.
7. User Installed Software (SA-7): EDD does not enforce explicit rules governing the installation of software by users.
8. Security Engineering Principles (SA-8): EDD does not design and implement the information system using security engineering principles.
9. External Information System Services (SA-9): EDD does not: (i) require that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.
10. Developer Security Testing (SA-11): EDD does not require that information system developers create a security test and evaluation plan, implement the plan, and document the results.

RISK: Strong system and services acquisition policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong system and services acquisition policy and procedures, EDD does not have a standardized approach to formally document and implement system and services acquisition policy and procedures.

Outsourced information system services protect information systems from unauthorized access by third-party providers.

Weak outsourced information services do not conform to the Agency's security policies; therefore, inadequate levels of information security may be implemented on the system, potentially allowing unauthorized access.

RECOMMENDATION: EDD Management should:

1. SA-1 System and Services Acquisition Policy and Procedures: Ensure the system services and acquisition policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.
2. SA-2 Allocation of Resources: EDD management should determine security requirements for the information system in mission/business case planning. A discrete line item for information system security should be established in EDD's programming and budgeting documentation.
3. SA-3 Life Cycle Support: EDD management should manage the information system using a system development life cycle methodology that includes information security considerations.
4. SA-4 Acquisitions: Acquisition contracts for information systems should include, either explicitly or by reference, security requirements and/or security specifications that describe:
    a. -required security capabilities;
    b. -required design and development processes;
    c. -required test and evaluation procedures; and
    d. -required documentation.
5. SA-5 Information System Documentation: EDD management should obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.
6. SA-6 Software Usage Restrictions: EDD management should comply with software usage restrictions.
7. SA-7 User Installed Software: EDD management should enforce explicit rules governing the installation of software by users.
8. SA-8 Security Engineering Principles: EDD management should maintain the information system using security engineering principles consistent with NIST SP 800-27 and ensure developers are trained in how to develop secure software.
9. SA-9 External Information System Services: Ensure third-party providers are subject to the same information system security policy and procedures of the supported agency, and must conform to the same security control and documentation requirements as would apply to EDD's internal systems. Appropriate Agency officials approve outsourcing of information system services to third-party providers (e.g., service bureaus). The outsourced information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service level agreements. A service level agreement should be developed and approved that defines the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.
10. SA-11 Developer Security Testing: EDD management should require that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results for newly developed systems and modifications to existing systems that impact security controls.

AGENCY REPONSE: The EDD is in compliance with SA-1 through SA-4, and SA-8. The EDD's Mobile Computing Security Encryption Policy and Personal Computer Acquisition and Replacement Policy, along with policy issued by the Department of General Services establishes the framework that the EDD uses for System and Service Acquisition, Allocation of Resources, Life Cycle Support, Acquisitions, and Security Engineering Principles.

The EDD is in compliance with SA-6 and SA-7. Software usage is controlled and monitored utilizing the following automated tools: System Management Server - Microsoft, Active Directory (AD) - Microsoft, Trusted Enterprise Manager – Avatier, and Altiris - Symantec. A user is provided access to a specific information system at the desktop level via EDD's Employee Service Account Request (ESAR) process. This process requires that a desktop users' manager submit the ESAR to the Information Technology Branch (ITB) Service Desk. A Remedy ticket is then generated to ITB/Infrastructure Services Division whereby a user account is created with the requested authorization. The account is created in the AD and assigned to a 'global group' within the AD. Altiris manages the desktop image and software by using an enterprise software packaging and deployment approach. The EDD controls the desktop configuration/image via a Corporate (base) image and a Business Layer image for each user within EDD's enterprise. Desktop users do not have systems administrator or desktop administrator rights and privileges. Therefore, they cannot make changes or download software to their desktop workstations. If a device is identified via desktop monitoring/auditing of being non compliant with EDD's core image, that device will be re-imaged to meet departmental standards/controls.

The EDD is in compliance with SA-8 through SA-10 by our Change Management Policy, which sets and defines EDD's configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation. An Infrastructure Change Control Board meets weekly to review Change Requests. Some of the areas covered by the change requests are testing and security.

(See Attachments 11, 12, and 13)

IRS COMMENT: Agency response is partially accepted. Recommendations for SA-5 and SA-11 are not addressed in the agency response. Mitigating actions for SA-5 should be corrected within twelve months after receiving the Final SRR. Mitigating actions for SA-11 should be corrected within three months after receiving the Final SRR. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Management Controls – Certification & Accreditation

H.4 **FINDING:** Certification & Accreditation controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, seven Certification & Accreditation controls were found to not be compliant with IRS Publication 1075 standards. The non-compliant controls under the Certification & Accreditation control family include:

1. Certification, Accreditation, and Security Assessment Policies and Procedures (CA-1): EDD does not develop, disseminate, and periodically review/update: (i) formal, documented, security assessment policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and associated assessment controls.
2. Security Assessments (CA-2): EDD does not conduct an assessment of the security controls in the information system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
3. Information System Connections (CA-3): EDD does not authorize all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.
4. Security Certification (CA-4): EDD does not conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
5. Plan of Action and Milestones (CA-5): EDD does not develop and update a plan of action and milestones for the information system that documents the Agency's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls to reduce or eliminate known vulnerabilities in the system.
6. Security Accreditation (CA-6): EDD does not authorize (i.e., accredit) the information system for processing before operations and update the authorization at least every three years or when there is a significant change to the system. A senior organizational official does not sign and approve the security accreditation.
7. Continuous Monitoring (CA-7): EDD does not ensure continuous monitoring is ongoing at all times. Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. EDD management should establish the selection criteria for control monitoring and subsequently select a subset of the security controls employed within the information system for purposes of continuous monitoring.

RISK: Strong security assessment policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong security assessment policy and procedures, EDD does not have a standardized approach to formally document and implement these assessment policy and procedures.

Security assessments can include compliance testing and security risk assessments, which are performed on the system every three years or when there is a major change to the system. In addition, on an annual basis, a self-assessment is conducted on the system to evaluate its management, operational, and technical controls.

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation. It details the risks that are facing the system and to what extent the security controls are effective in mitigating those risks. Without a security certification, Agency officials lack the facts needed to render an accurate security accreditation decision.

A Plan of Action and Milestones (POA&M) is developed for systems to document the planned, implemented, and evaluated remedial actions to correct deficiencies identified during the assessment of the security controls in order to reduce or eliminate known vulnerabilities. Without a POA&M, corrective actions cannot be efficiently tracked and progress monitored for the system, thereby increasing the potential for weak system security.

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Without a system accreditation, Agency officials may not be fully aware of the security risks, technical constraints, operational constraints, and cost/schedule constraints facing a system, and therefore may not account for any adverse impacts to EDD if a breach of security occurs.

Continuous monitoring ensures that the system security controls are current and effective to address all current and newly identified threats and vulnerabilities. Without continuous monitoring, which includes configuration management activities and ongoing annual self-assessment of security controls, EDD may not have current evaluations of the system security controls implemented to protect against existing and future threats and vulnerabilities.

RECOMMENDATION: EDD management should:

1. CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures: Develop security assessment policy and procedures that are

consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The security assessment policies can be included as part of the general information security policy for the Agency. Security assessment procedures can be developed for the security program in general, and for a particular information system, when required.

2. CA-2 Security Assessments: Develop security assessments to support the requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be tested with a frequency depending on risk, but no less than annually.
3. CA-3 Information System Connections: EDD management should authorize all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.
4. CA-4 Security Certification: EDD management should conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Ensure the process is consistent with OMB policy and NIST Special Publications 800-37 and 800-53A.
5. CA-5 Plan of Action and Milestones: EDD management should ensure a POA&M is developed/updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M is a key document in the security package developed, and the POA&M is reviewed at least quarterly to address the elimination or acceptance of all risks identified.
6. CA-6 Security Accreditation: EDD management should authorize/accredit the information system for processing before operations and update the authorization in accordance with organization-defined frequency, at least every three years. Ensure a senior organizational official signs and approves the security accreditation. Ensure security accreditation process employed by the organization is consistent with NIST Special Publications 800-37 and that EDD updates the authorization when there is a significant change to the information system.
7. CA-7 Continuous Monitoring: EDD management should ensure continuous monitoring is ongoing at all times. Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. EDD establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring.

AGENCY REPONSE: The EDD is aware of the National Institute of Standards and Technology (NIST) Certification and Accreditation safeguard and controls for Information Technology Systems. The EDD's published audit and information security policy for ERM Framework includes the following standards: the EDD

Information Technology Governance Council adopted ERM best practices set forth by the Committee of Sponsoring Organizations (COSO) and the NIST for EDD's risk assessments and internal audit preparedness processes. The COSO standards are being used for programmatic portion of the risk assessments and the NIST standards are being used for IT portion of the risk assessments. The policy includes the Federal Information Security Management Act and the Federal Office of Management and Budget Circular A130-Appendix III.

(See Attachment 2)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Personnel Security

H.5 **FINDING**: Personnel Security controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: During an interview with a Human Resources representative it became clear that the department is following State of California agreements with its unions covering the matters of personnel handling. These procedures do not allow for sufficient investigation and suitability requirements for individuals with access to FTI data. The department did produce evidence of a suitable policy for termination and transfer of individuals with FTI access.

1. Personnel Security Policy and Procedures (PS-1): EDD does not develop, disseminate, nor periodically review/update: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
2. Position Categorization (PS-2): EDD does not assign a risk designation to all positions nor establish screening criteria for individuals filling those positions.
3. Personnel Screening (PS-3): EDD does not fully screen individuals requiring access to organizational information and information systems before authorizing access.
4. Personnel Sanctions (PS-8): EDD does not employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

RISK: Absent or weak personnel security policy and procedures could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system.

Absent or weak position categorization and personnel screening prevents EDD from determining that the appropriate personnel are assigned to the appropriate roles. Weak position categorization and personnel screening may potentially allow unauthorized access to the information system and the information.

Personnel screening helps the Agency determine the appropriate personnel are assigned to the appropriate roles. Weak personnel screening may potentially allow unauthorized access to the information and the information system.

An organization without a formal process for applying sanctions for individuals failing to comply with established information security policies and procedures promotes a general attitude that information security practices are of little importance to the individuals well being. Once that attitude is set in an individual or organization the discipline needed to produce a secure environment is gone and individuals will have little reason to comply with security requirements that cause extra work and extra efforts.

RECOMMENDATION: EDD Management should:

1. PS-1: Develop personnel security policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for EDD. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required.
2. PS-2: Ensure that position risk designations are consistent with applicable policy and guidance.
3. PS-3: Ensure that personnel screening is consistent with applicable policy, regulations, and guidance and the criteria established for the risk designation of the assigned position.
4. PS-8: The policy and rules of behavior documents should contain a formal sanctions process for personnel failing to comply with EDD information security policies and procedures.

AGENCY REPONSE: The EDD is in compliance with PS-1 through PS-3 and PS-8. The EDD provides annual training for all staff to ensure compliance.

(See Attachment 14)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Contingency Planning

H.6 **FINDING**: According to the on-site evaluation performed contingency planning controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: The agency did not produce evidence of contingency planning.

1. Contingency Planning Policy And Procedures (CP-1):
    a. Contingency planning policy and procedures do not (i) exist; (ii) are not documented; (iii) and not disseminated to appropriate elements within EDD.

   b. Contingency planning policy and procedures are not (i) periodically reviewed by responsible parties within EDD; and (ii) are not updated, when EDD review indicates updates are required.
   c. Contingency planning policy does not address the following areas: Alternate Storage Sites, Telecommunication Services, and Information System Backup.
2. Contingency Plan (CP-2):
   a. The ITCP does not address contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34.
   b. The contingency plan is not reviewed and approved by designated organizational officials, and disseminated to key personnel with contingency planning responsibility.
3. Contingency Plan Testing(CP-4):
   a. EDD does not define a set of contingency plan tests and/or exercises, and test/exercise the contingency plan annually.
   b. Testing records, such as after action reports, are not created to document the results of contingency plan testing/exercise. The ITCP is not updated based on the results of the test/exercise.
4. Contingency Plan Update (CP-5): EDD does not review the contingency plan for the information system.
5. Alternate Storage Site(CP-6): EDD did not identify an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
6. Alternate Processing Site(CP-7): EDD did not identify an alternate processing site and the necessary agreements to permit the resumption of information systems operations for critical mission functions within EDD.

RISK: Strong contingency planning policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong contingency planning policy and procedures, EDD does not have a standardized approach to formally document and implement contingency planning policy and procedures.

RECOMMENDATION: EDD Management should:

1. CP-1: Contingency Planning Policy And Procedures
   a. Contingency planning policy and procedures should (i) exist; (ii) be documented; (iii) and be disseminated to appropriate elements within EDD.
   b. Contingency planning policy and procedures should (i) be periodically reviewed by responsible parties within EDD; and (ii) be updated, when EDD review indicates updates are required.

c. Contingency planning policy should address the following areas: Alternate Storage Sites, Telecommunication Services, and Information System Backup.

2. CP-2: Contingency Plan:
   d. The ITCP should address contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34.
   e. The contingency plan should be reviewed and approved by designated organizational officials, and disseminated to key personnel with contingency planning responsibility.
3. CP-4: Contingency Plan Testing:
   f. EDD management should define a set of contingency plan tests and/or exercises, and test/exercise the contingency plan annually.
   g. Testing records, such as after action reports, should be created to document the results of contingency plan testing/exercise. The ITCP should be updated based on the results of the test/exercise.
4. CP-5 Contingency Plan Update: EDD management should review the contingency plan for the information system.
5. CP-6 Alternate Storage Site: EDD management should identify an alternate storage site and initiate necessary agreements to permit the storage of information system backup information.
6. CP-7 Alternate Processing Site: EDD management should identify an alternate processing site and the necessary agreements to permit the resumption of information systems operations for critical mission functions within EDD.

AGENCY REPONSE: The EDD is in compliance with findings CP-1 through CP-7, as indicated below:

CP-1: Contingency Planning Policy and Procedures:

a. Continuity Plan For Business (CPB) Policy and Procedures do exist, are documented, and are disseminated to all appropriate branches within the EDD. The ISO is responsible for this implementation.
b. Contingency planning policy and procedures are periodically reviewed by the responsible parties within the EDD and are updated every May, in accordance with procedures as outlined by the ISO. The ISO is responsible for this implementation.
c. Contingency planning policy does address Alternate Storage Sites, Telecommunication Services, and Information System Backup. This information is located in Section 5 of the Enterprise CPB. The ISO is responsible for this implementation.

CP-2: Contingency Plan:

d. The ITB CPB outlines contingency roles, responsibilities, assigns individual with contact information and all activities for restoring the information systems consistent with the NIST Special Publication 800-34. This information is located in Section 5 of the Enterprise CPB for

the EDD. The ITB Continuity Management Office (CMO) has responsibility for this implementation.

e. The ITB CPB is updated yearly in May and reviewed for approval by the ISO, the ITB Deputy Director and all ITB Division Chiefs. The finalized ITB CPB is then disseminated to all key personnel including the ITB Deputy Director's Office, all ITB Division Chiefs, all Disaster Recovery Team leaders, and key team members. The ITB CMO has responsibility for this implementation.

CP-4: Contingency Plan Testing:

f. The EDD performs a yearly test of the hot site and ITB CPB in conjunction with the DTS. All major portions of the ITB CPB are tested for accuracy and effectiveness. Also smaller tests are scheduled annually outside the hot site test to highlight different portions of the ITB CPB for effectiveness review. The ITB CMO has responsibility for this implementation.

g. Testing records and Post Warm site Exercise Report was disseminated to all appropriate people for review and comment after the hot site test. Lessons learned from the report will be incorporated into the ITB CPB. The ITB CMO has responsibility for this implementation.

CP-5: Contingency Plan Update:

The ITB CPB is sent to the ITB Deputy Director and all ITB Division Chiefs for review, additions and comments before the final edition is disseminated to Recovery Team personnel. The ITB CMO has responsibility for this implementation.

CP-6: Alternate Storage Site:

The EDD currently has a contract with Iron Mountain through the DTS to provide secure off-site storage of our information system backups.

(See Attachment 19)

CP-7: Alternate Processing Site:

The EDD currently has a contract with International Business Machines through the DTS to provide an off-site processing site in Boulder, Colorado. In addition, the EDD central office has a contingency plan with the Tax Branch to provide an Alternate Work Site in the event that EDD's main offices in downtown Sacramento are unavailable for use due to disaster.

(See Attachment 20)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Configuration Management

H.7 **FINDING**: According to the on-site evaluation performed configuration management controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, five of the eight Configuration Management controls were found to not be compliant with IRS Publication 1075 standards. The five non-compliant controls under the Configuration Management control family include:

1. Configuration Management Policy and Procedures (CM-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
2. Monitoring Configuration Changes (CM-4): EDD does not monitor changes to the information system by conducting security impact analyses to determine the effects of the changes.
3. Configuration Settings (CM-6): EDD does not configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements. For example, the Mainframe with Top Secret had a number of configuration findings that are not consistent with IRS Publication 1075's recommendations.
4. Least Functionality (CM-7): EDD does not configure the information system to provide only essential capabilities and does not specifically prohibit and/or restrict the use of the functions, ports, protocols, and/or services EDD has determined are unacceptable risks.
5. Information System Component Inventory (CM-8): EDD has not developed, documented, or maintained a current inventory of the components of the information system with relevant ownership information.

RISK: Strong configuration management policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong configuration management policy and procedures, EDD does not have a standardized approach to formally document and implement configuration management policy and procedures.

Failure to analyze proposed or actual changes to the information system and determine the security impact of such changes before they are implemented may affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously.

Security configuration settings that ensure the system is configured to the most restrictive mode possible prevent unauthorized users from making unapproved changes to the system, thereby protecting system integrity. Lack of mandatory security configuration settings may result in exploitation without detection or user accountability.

Lack of access restriction may result in exploitation without detection or user accountability.

Lack of configuration settings may result in exploitation without detection or user accountability.

Least functionality settings closes all non-essential functionalities and services (e.g., prohibited or unused ports, protocols, services, voice over internet protocol, instant messaging, file transfer protocol, hyper text transfer protocol, file sharing, etc.). Failure to set systems to least functionality may increase system vulnerabilities and expose the system to malicious attacks.

RECOMMENDATION: EDD Management should:

1. CM-1 Configuration Management Policy and Procedures: Develop configuration management policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for EDD. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required.
2. CM-4 Monitoring Configuration Changes: EDD management should monitor changes to the information system by conducting security impact analyses to determine the effects of the changes.
3. CM-6: Configuration Settings: EDD management should ensure EDD records or documents show that the system is configured as follows: (i) mandatory configuration settings for information technology products employed within the information system are established; (ii) security settings of information technology products are configured to the most restrictive mode consistent with operational requirements; (iii) configuration settings are documented; and (iv) configuration settings in all components of the information system are enforced.
4. CM-7 Least Functionality: EDD management should ensure the system provides only the essential capabilities and prohibits any functionality that is not essential. Specifically the following protocols/services shall be disabled: (i) Network File System, (ii) Network Information System, (iii) Remote Procedure Call (RPC), (iv) Trivial File Transfer Protocol (TFTP), (v) User Datagram Protocol (UDP), (vi) boot services, (vii) r-commands, (viii) Routing Information Protocol (RIP), (ix) daemon (routed), and (x) Internet Control Message Protocol (ICMP) redirects. Ensure all prohibited ports, protocols, and services are disabled.

5. CM-8 Information System Component Inventory: EDD management should develop, document, and maintain a current inventory of the components of the information system with relevant ownership information.

AGENCY REPONSE: The EDD is in compliance with CM-1 through CM-8. The EDD's Production Change Management Process covers all aspects of Configuration Management, Configuration Changes, and Configuration Settings. Least Functionality (CM-7) is addressed in EDD's Production Change Management Process and in EDD's Information Security Policy. Information System Component Inventory (CM-8) is developed, documented, and maintained by the EDD's Cost and Resources Management Section and the Enterprise Architecture Office.

(See Attachments 16 and 8)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Maintenance

H.8 **FINDING**: According to the on-site evaluation performed maintenance controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, three of the eight Maintenance controls were found not to be compliant with IRS Publication 1075 standards. The three non-compliant controls under the Configuration Management control family include:

1. System Maintenance Policy and Procedures (MA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
2. Maintenance Tools (MA-3): EDD does not approve, control, and monitor the use of information system maintenance tools nor maintain the tools on an ongoing basis.

3. Remote Maintenance (MA-4): EDD does not approve, control, and monitor remotely executed maintenance and diagnostic activities. Telnet is used for remote maintenance of the system. Additionally, the vendor can remotely access the system through the telephone directly connected to the mainframe.

RISK: Strong system maintenance policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong system maintenance policy and procedures, the Agency does not have a

standardized approach to formally document and implement system maintenance policy and procedures.

The use of approved maintenance tools on an ongoing basis helps to ensure information system equipment continues to operate correctly. Without proper maintenance tools, the risk of unauthorized or inappropriate changes to the equipment or system increases.

Remote maintenance controls help ensure any remotely executed maintenance and diagnostic activities are performed in accordance with all Agency maintenance policy and procedures. Weak remote maintenance controls may potentially allow unauthorized access to the information system or the information the system processes, stores, or transmits.

RECOMMENDATION: EDD management should:

1. MA-1 System Maintenance Policy and Procedures: Develop information system maintenance policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the Agency. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required.
2. MA-3 Maintenance Tools: Ensure all maintenance tools policy and procedures adequately address the use of maintenance tools. Ensure that maintenance tools used to perform system maintenance are approved and use of the tools is monitored.
3. MA-4 Remote Maintenance: Ensure EDD approves, controls, and monitors remotely executed maintenance and diagnostic activities. Maintenance logs are maintained for all remote maintenance, diagnostic, and service activities. Appropriate Agency officials periodically review maintenance logs. When remote maintenance is completed, the information system should terminate all sessions and remote connections. Telnet is not used for remote maintenance.

AGENCY REPONSE: The EDD is in compliance with MA-1 through MA-4. System Maintenance, Maintenance Tools, and Remote Maintenance are covered in EDD's Information Security Policy and the Employee Access Control Policy.

(See Attachments 8 and 17)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – System and Information Integrity

H.9 **FINDING:** System & Information Integrity controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, six System and Information Integrity controls were found not to be compliant with IRS Publication 1075 standards. The six non-compliant controls under the System and Information Integrity control family include:

1. System And Information Integrity Policy And Procedures (SI-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
2. Malicious Code Protection (SI-3): EDD does not implement malicious code protection.
3. Information System Monitoring Tools and Techniques (SI-4): EDD does not employ tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.
4. Security Alerts and Advisories (SI-5): EDD does not receive information system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.
5. Information Input Restrictions (SI-9): EDD does not restrict the capability to input information into the system to authorized individuals.
6. Information Output Handling and Retention (SI-12): EDD does not handle and retain output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

RISK: Strong system and information integrity policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong system and information integrity policy and procedures, EDD does not have a standardized approach to formally document and implement system and information integrity policy and procedures.

Information system monitoring tools and techniques help to detect any system intrusions. Without employing appropriate monitoring tools and techniques, the information system may be slow to detect intrusions and become more vulnerable to attacks.

Failure to receive information system security alerts/advisories on a regular basis may hamper the Agency's ability to improve knowledge of security best practices and react accordingly to mitigate exploitable vulnerabilities.

RECOMMENDATION: EDD Management should:

1. SI-1 System and Information Integrity Policy and Procedures: EDD management should develop system and information integrity policy and procedures that are consistent with the IRS Publication 1075 and applicable

federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for EDD. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required.

2. SI-2 Malicious Code Protection: EDD management should ensure a process is in place to identify recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the system. Ensure newly released security patches, service packs and hot fixes are installed on the information system in a reasonable timeframe in accordance with agency policy and procedures, and after being tested in a test environment.
3. SI-3 Information System Monitoring Tools and Techniques: EDD management should ensure EDD employs virus protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network that store, process or transmit FTI. Ensure virus protection mechanisms are configured to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) transported: by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means. Ensure the virus protection mechanisms (including the latest virus definitions) are updated whenever new releases are available, and the virus protection mechanism automatically updates its malicious code definitions. Ensure consideration is given to using virus protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).
4. SI-4 Security Alerts and Advisories: EDD management should ensure the information system has intrusion detection capability. The intrusion detection tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signature, and traffic anomalies.
5. SI-9 Information Input Restrictions: EDD management should ensure restrictions are employed for personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities. User accounts should be restricted from inputting information beyond the typical access controls unless specifically authorized based on operational/project responsibilities.
6. SI-12 Information Output Handling and Retention: EDD management should ensure EDD retains output from the information system in accordance with Agency policy and operational requirements/procedures. EDD management should handle output from the information system according to the system marked instructions and Agency policy and operational procedure and operational requirements/procedures.

AGENCY REPONSE: The DTS implements "Malicious Code Protection," including protection from viruses, worms, Trojan horses, and spyware, at various points in the network infrastructure and on applicable hosts. The DTS deploys malicious code protection that blocks incoming malicious e-mail at the email gateways. The DTS deploys host-based malicious code protection on Windows

servers and desktops. The DTS does not deploy malicious code protection on those platforms where it is not considered a significant threat (e.g. UNIX including AIX, and Z/OS). The DTS' Intrusion Prevention System (IPS) also blocks some malicious codes. The specific IPS protection varies depending on the network location.

The DTS has a proactive detection and remediation program for security vulnerabilities. When advisories are received they are analyzed and systems updated if appropriate. This is documented in DTS' policy "3300 Vulnerability Management Policy."

(See Attachment 7)

IRS COMMENT: Agency response is partially accepted. The agency's response does not address SI-9 or SI-12. SI-9 mitigating recommendations should be corrected within six months after receiving the Final SRR. SI-12 mitigating recommendations should be corrected within three months after receiving the Final SRR. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Operational Controls – Incident Response and Incident Reporting

H.10 FINDING: Incident Response and Incident Reporting controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, seven of the Incident Response and Incident Reporting controls were found to not be compliant with IRS Publication 1075 standards. The seven non-compliant controls under the Incident Response and Incident Reporting control family include:

1. Incident Response Policy and Procedures (IR-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
2. Incident Response Training (IR-2): EDD does not train personnel in their incident response roles and responsibilities with respect to the information system and does not provide refresher training annually.
3. Incident Response Testing and Exercises (IR-3): EDD does not test and/or exercise the incident response capability for the information system annually using Agency-defined tests and/or exercises to determine the incident response effectiveness and document the results.
4. Incident Handling (IR-4): EDD does not implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

5. Incident Monitoring (IR-5): EDD does not track and document information system security incidents on an ongoing basis.
6. Incident Reporting (IR-6): EDD does not promptly report incident information to appropriate authorities.
7. Incident Response Assistance (IR-7): EDD does not provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

RISK: Strong incident response policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong incident response integrity policy and procedures, EDD does not have a standardized approach to formally document and implement incident response policy and procedures.

Incident response training provides necessary instructions to personnel when security incidents need to be reported. Failure to provide incident response training may prevent effective and efficient reporting efforts of security breaches. Failure to test and/or exercise the incident response capability may hamper the Agency's ability to be prepared for actual emergency situations related to the IT plan.

Lack of a well developed incident handling policy cripples an Agency's ability to best respond to and manage adverse situations involving the information system. Incident handling policies and procedures will promote more efficient utilization of capabilities in responding to cyber attacks.

Incident monitoring ensures inappropriate or unusual activity is reported to management, local security personnel, and network security and the incident is appropriately documented and tracked. Failure to provide incident monitoring controls may prevent effective and efficient reporting efforts of security breaches.

Lack of a well developed incident reporting policy cripples an Agency's ability to best respond to and manage adverse situations involving the information system. Incident reporting policies and procedures will promote more efficient utilization of capabilities in responding to cyber attacks.

Incident response assistance provides a way for users to report incidents and for the appropriate response and assistance to be provided to aid in recovery.

RECOMMENDATION: EDD management should:

1. IR-1 Incident Response Policy and Procedures: Develop incident response policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the Agency. Incident response

procedures can be developed for the security program in general, and for a particular information system, when required.

2. IR-2 Incident Response Training: Ensure personnel are trained on their incident response roles and responsibilities. EDD management should ensure inappropriate or unusual activity is reported to management, local security personnel, and network security.
3. IR-3 Incident Response Testing and Exercises: EDD management should test and exercise the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency. Ensure tests/exercise results are documented. NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.
4. IR-4 Incident Handling: Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly. Ensure the incident handling capability is consistent with NIST Special Publication 800-61. NIST Special Publication 800-83 provides guidance on Malware incident handling and prevention.
5. IR-5 Incident Monitoring: Ensure that personnel are provided mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. Ensure all incidents are appropriately documented and progress tracked.
6. IR-6 Incident Reporting: Ensure weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. Ensure the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. NIST Special Publication 800-61 provides guidance on incident handling and reporting.
7. IR-7 Incident Response Assistance: Provide an incident response support resource that offers advice and assistance to information system users. Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

AGENCY REPONSE: The EDD is in compliance with IRS' recommendation regarding the policies for handling, monitoring, and reporting incidents and the response to the incident.

(See Attachment 18)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Awareness and Training

H.11 FINDING: Security training and awareness controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, one of four Awareness and Training controls were found to be compliant with IRS Publication 1075 standards. The three non-compliant controls under the Incident Response and Incident Reporting control family include:

1. Security Awareness and Training Policy And Procedures (AT-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
2. Security Awareness (AT-2): EDD does not ensure all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and annually thereafter.
3. Security Training (AT-3): EDD does not identify personnel with significant information system security roles and responsibilities, document those roles and responsibilities, and provide appropriate information system security training before authorizing access to the system and annually thereafter.

RISK: Strong security awareness and training policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong security awareness and training policy and procedures, EDD does not have a standardized approach to formally document and implement security awareness and training policy and procedures.

Security awareness provides personnel and contractor employees involved with the management, operation, programming, maintenance, or use of Agency information systems with the necessary security basics to promote a responsible and secure operating environment. Weak security awareness controls may potentially allow unauthorized access (intentional or unintentional) to the information system or the information the system processes, stores, or transmits.

Security training controls provides personnel and contractor employees involved with the management, operation, programming, maintenance, or use of Agency information systems with the necessary security basics to promote a responsible and secure operating environment. Without formally documented and established roles and responsibilities, appointed personnel may not know or fully understand their expectations and/or functional limitations. Weak security training controls may potentially allow unauthorized access (intentional or unintentional) to the information system or the information the system processes, stores, or transmits.

RECOMMENDATION: EDD management should:

1. AT-1 Security Awareness and Training Policy and Procedures: Develop security awareness and training policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the Agency. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required.
2. AT-2 Security Awareness: Ensure the development of appropriate security awareness content and training material based on the specific requirements of EDD and the information system to which personnel have authorized access. Conduct the security awareness training before the users can access the information systems and continue annually thereafter. EDD management should determine the appropriate content of security awareness training based on the specific requirements of EDD and the information systems to which personnel have authorized access.
3. AT-3 Security Training: Identify appropriate personnel with significant information system security roles and responsibilities. Document those roles and responsibilities, and conduct appropriate information system security training before authorizing access to the system, and periodically conduct the security training thereafter. EDD management should determine the appropriate content of security training based on the specific requirements of EDD and the information systems to which personnel have authorized access. In addition, EDD management should ensure system managers, system administrators, and other personnel who have access to system-level software have adequate technical training to perform their assigned duties.

AGENCY REPONSE: The EDD is in compliance with IRS' recommendation.

(Refer to D.1 of the IRS Safeguard Review Report dated June 2008.)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technical Controls – Identification and Authentication

H.12 **FINDING**: Identification and authentication controls are implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, five of the Identification and authentication controls were found not to be compliant with IRS Publication 1075 standards.

1. Identification And Authentication Policy And Procedures (IA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented

procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

2. Device Identification and Authentication (IA-3) EDD's information system does not identify and authenticate specific devices before establishing a connection.
3. Identifier Management (IA-4): EDD does not manage user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate Agency official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after 90 days of inactivity; and (vi) archiving user identifiers. User account management policy and procedures do not exist but informal processes seem to be in place.
4. Authenticator Management (IA-5): EDD does not manage information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authentication distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.
5. Cryptographic Module Authentication (IA-7): The EDD information system does not employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

RISK: Strong identification and authentication policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong identification and authentication policy and procedures, the Agency does not have a standardized approach to formally document and implement identification and authentication policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

Identifier management allows an Agency to protect itself from possible exploitation of the identifier creation process. Failure to implement this security control could lead to unauthorized access to the information system resulting in irreversible and detrimental harm to information system data, users and assets.

RECOMMENDATION: EDD management should:

1. IA-1 Identification And Authentication Policy and Procedures: Develop identification and authentication policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the Agency. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required.

2. IA-3 Device Identification and Authentication: EDD's information system should identify and authenticate specific devices before establishing a connection.
3. IA-4 Identifier Management: Establish an identifier management procedure to:
   1) Uniquely identify each user;
   2) Verify the identify of each user;
   3) Designate appropriate Agency officials that shall issue authorizations for the establishment of information system user accounts;
   4) Ensure that the user identifier and information system access credentials are issued to the intended party in such a manner so as to prevent compromising the confidentiality of the credentials;
   5) To disable user access to the information system after a 90 day period of inactivity;
   6) Assure that user identifiers are archived, and that those archives are kept secure.
4. IA-5 Authenticator Management: EDD management should manage information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authentication distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.
5. IA-7 Cryptographic Module Authentication: The EDD information system should employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

AGENCY REPONSE: The EDD has a documented Employee Access Control Policy. The policy addresses the purpose, scope, responsibilities, standards, and requirements. This policy is provided to program managers, system and network administrators, system application developers, and EDD staff. The policy discusses a uniform, consistent approach to design, implement, and maintain data integrity and information security in systems and applications.

The EDD is in compliance with IRS' recommendation. The EDD prohibits the use of external connections such as modems, wireless networks, dialup connections, wireless devices, etc. without written approval from the ITB Deputy Director and Information Security Officer. The approval is based on a risk analysis, risk mitigation plan, and individual authentication plan that ensure appropriate information security. (Reference: EDD Employee Access Control Policy – pg.6)

Numbers 1-4 – The EDD is in compliance with IRS' recommendation. All individuals provide identification and authentication in the form of a unique Identification (UserID) and password before accessing EDD sensitive or confidential information. The EDD prohibits the use of group and shared passwords. (Reference: EDD Employee Access Control Policy – pg.7)

Number 5 – The EDD is in compliance with IRS' recommendation. (Reference: Information Systems Standards and Procedures Manual – UserID standards [Screen 10])

- The UserID that has never been used will be deleted after 3 months;
- The UserID that has not had any activity for 90 days will be automatically inactivated.

(See Attachment 17)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technical Controls – Access Control

H.13 **FINDING**: According to the on-site evaluation performed access controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, seven of the Identification and authentication controls were found not to be compliant with IRS Publication 1075 standards.

1. Access Control Policy and Procedures (AC-1): EDD management has not developed, disseminated, or reviewed (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
2. Account Management (AC-2): EDD does not manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. EDD does not review information system accounts at lest annually.
3. Least Privilege (AC-6): The EDD information system does not enforce the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
4. Unsuccessful Login Attempts (AC-7): The EDD information system does not enforce a limit of 3 consecutive invalid access attempts by a user during a 15 minute time period. The information system does not automatically lock the account for a 15 minute time period, nor delay the next login prompt for 15 minutes when the maximum number of unsuccessful attempts is exceeded.
5. System Use Notification (AC-8): The EDD information system does not display an approved system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring. The system use notification message does not provide appropriate privacy and security notices based on IRS requirements.

6. Session Lock (AC-11): The EDD information system does not prevent further access to the system by initiating a session lock after 15 minutes of inactivity until the authorized user reestablishes access using appropriate identification and authentication procedures.
7. Session Termination (AC12): The EDD information system does not automatically terminate a remote session after 15 minutes of inactivity.

RISK: Strong access control policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong access control policy and procedures, the Agency does not have a standardized approach to formally document and implement access control policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

Managing information system accounts - to include the individual aspects of the management process - are essential to the security of the information system as it allows administrators to restrict access solely to authorized parties, identify who those parties are, and to exercise authority over the security controls governing the access restrictions of these parties. Failure to manage information system accounts or review them on a frequent basis can result in unauthorized access to information system resources and eliminate any ability to enforce accountability for information system misuse. Failure to employ automated mechanisms to support the management of information system accounts increases the possibility of human error. Failure to automatically terminate temporary and emergency accounts, or to automatically disable inactive accounts after a period of time can result in unauthorized access through exploitation of these accounts. Because these accounts are not periodically reviewed, the unauthorized access will continue indefinitely.

Enforcing the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks mitigates the risk that authorized personnel are conducting unauthorized activities on or with the information system. Failure to enforce the most restrictive set of rights/privileges for users on the information system can lead to exploitation and compromise of the security and functionality of the information system.

Enforcing a limit on the number of consecutive access attempts by a user within a time period which would result in temporary lockout when the limit is met assures that unauthorized users attempting to access authorized users' information system accounts are prevented from doing so. Failure to enforce a limit on the number of consecutive access attempts by a user can facilitate an unauthorized user's attempts to "brute force" their way into an authorized user's account by guessing an indefinite number of passwords until the valid one is uncovered.

Displaying an approved system use notification message which informs potential users that the information system is the property of the U.S. Government, that usage on it may be monitored, that unauthorized use of the system may result in criminal or civil penalties, and that use of the system indicates consent to monitoring, informs the end user of the responsibilities they have when accessing the system and when using it, and of the consequences of unauthorized access or use of the information system. Without this banner, Agencies may have no legal recourse to monitor an end user's actions or discipline an end user for violating the Agency's rule of behavior.

Documenting, monitoring and controlling all methods of remote access to the information system is necessary in that it applies the same level of security protection to forms of remote access as are implemented on forms of local access. Failure to document, monitor and control all methods of remote access leaves the information system vulnerable to attack from an outside unauthorized party. Failure to employ automated mechanisms to facilitate the monitoring and control of remote access methods leaves the information system vulnerable to human error. Failure to use encryption to protect the confidentiality of remote access sessions can result in data interception by an unauthorized third-party eavesdropping on a remote connection between the information system and an authorized user. Failure to control all remote accesses through a managed access control point creates difficulty in assuring that all remote accesses are subject to the same level of security.

Terminating a session after a period of inactivity is necessary in that it decreases the possibility that an unauthorized user will seize control of the session. Failure to terminate a session after a period of inactivity makes it likely that a passing user might take control of the session on the device that has been apparently abandoned and have access to FTI data.

RECOMMENDATION: EDD Management should:

1. AC-1: Develop access control policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for EDD. Access control procedures can be developed for the security program in general, and for a particular information system, when required.
2. Account Management (AC-2): Minimize manual review processes and decrease risk by implementing system-based controls that:
    a. automatically disables inactive and accounts after the account reaches the defined period of inactivity;
    b. automatically disables temporary accounts based on the defined period temporary accounts are permitted to exist.
3. Least Privilege (AC-6): EDD management should enforce the concept of least privilege by:
    a. Assign only the absolute minimum level of access necessary to users in order to conduct their tasks;

b. Develop a procedure so that authorization for any increase in functionality should come only through approved channels.

4. Unsuccessful Login Attempts (AC-7): The EDD information system should ensure that all information system accounts are configured to be disabled for a certain period of time, or until the authorized user contacts an official or Agency authorized to reinstate account access, in the event that a consecutive invalid access attempts is reached. If possible, enable a mechanism which would inform the user upon exceeding this limit, or upon further attempts to authenticate (or both) of how to reinstate account access.
5. System Use Notification (AC-8): The EDD information system should implement a system use notification message to be displayed before granting system access which informs users that the information system is the property of the U.S. Government, that use of the system may be monitored, that unauthorized use of the system may result in criminal or civil penalties, and that use of the system indicates consent to monitoring. Such language should be composed by general counsel, or the language provided in agency/department wide policy should state, that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and that use of the system indicates consent to monitoring. The message must be in accordance with stipulations in IRS Publication 1075.
6. Session Lock (AC-11): The EDD information system should implement a session lock that is activated after a defined period of computer inactivity and remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
7. Session Termination (AC12): The EDD information system should automatically terminate a remote session after 15 minutes of inactivity.

AGENCY REPONSE: When one's workstation is left unattended for an extended period, individuals must: (Reference: EDD Employee Access Control Policy – pg.
6)

a. Terminate active sessions when finished, unless they are secured by an appropriate locking mechanism; e.g., a password protected screen saver;
b. Secure personal computers (PC) or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use;
c. Use the "Lock Workstation" function anytime they leave their immediate areas (applies to Windows NT and 2000);
d. Individuals with workstations running Windows 95 must execute the "Shutdown-Log on as another individual" function anytime they leave their immediate work area; and
e. Follow instructions outlined in the Information Technology Circular (ITC) 01-08C "Re-issuance of the Desktop Security Screen Saver Feature Requirement."

The EDD has a documented Employee Access Control Policy that addresses consistent protection of data integrity and information security of all programs, systems, and business applications within the EDD. Before individuals are granted access rights, they must complete their information security training,

locally required training, and sign the appropriate nondisclosure agreements. Each automated information session must start with the person establishing their identity and authorizations (unique personal identifier and password).

(See Attachment 17)

IRS COMMENT: Agency response is partially accepted. The agency's response and the attachment do not adequately address the AC-2, AC-7, and AC-8 recommendations. AC-2, AC-7, and AC-8 recommended mitigations should be corrected within three months after receiving the Final SRR. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Technical Controls – Auditing

H.14 FINDING: Audit & Accountability controls are not being implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, six Audit & Accountability controls were found to not be compliant with IRS Publication 1075 standards. The non-compliant controls under the Audit & Accountability control family include:

1. Audit And Accountability Policy And Procedures (AU-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
2. Auditable Events (AU-2): The EDD information system does not generate audit records for the events as required in IRS Publication 1075.
3. Content Of Audit Records (AU-3): The EDD information system does not produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
4. Response To Audit Processing Failures (AU-5): The EDD information system does not alert appropriate organizational officials in the event of an audit processing failure and EDD has not defined the activities the system should take.
5. Audit Reduction And Report Generation (AU-7): The EDD information system does not provide an audit reduction and report generation capability.
6. Time Stamps (AU-8): The EDD information system does not provide time stamps for use in audit record generation.

RISK: Strong audit and accountability policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong audit

and accountability policy and procedures, EDD does not have a standardized approach to formally document and implement audit and accountability policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

RECOMMENDATION: EDD Management should:

1. AU-1 Audit And Accountability Policy And Procedures: Develop audit and accountability policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for DSS. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required.
2. AU-2 Auditable Events: Develop, document and continuously update a list of all auditable events. Configure the information system so that it can record these events per the IRS Publication 1075 policy. Include in this list of auditable events, procedures for compiling and distributed the audit records to the necessary parties for review.
3. AU-3 Content Of Audit Records: Develop and document a list of required information for auditing logging that provides sufficient information for the Agency to determine what occurred, the source, and the outcome of the events. Using this list, determine if this capability exists within the information system.
4. AU-5 Response To Audit Processing Failures: Provide sufficient storage capacity to capture records based on Agency guidance and best practices. In addition, configure automatic notifications are implemented and functional so that there is no failure in the notification of Agency officials in the event of an audit failure or storage capacity being reached.
5. AU-7 Audit Reduction and Report Generation: The EDD management should acquire an audit reduction and reporting tool.
6. AU-8 Time Stamps: Configure the audit logging functionality of the information system to include time stamps as part of the audit record (a good rule of thumb for the content of audit records is to ensure that "who", "what", "where", "when", and "how" are addressed). In addition, the Agency should configure all information systems to synchronize to a central NTP server so that one time is used for all IT assets with clocks.

AGENCY REPONSE: The EDD has established a concept to develop an Audit Logging program similar to the State of California's Franchise Tax Board. A Budget Change Proposal to authorize the necessary funds for this program is also under development. The EDD will provide the IRS with Quarterly updates regarding the status of this Corrective Action Plan.

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technical Controls – System & Communications Protection

H.15 FINDING: System & Communications Protection controls are not being implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, five System & Communications controls were found not to be compliant with IRS Publication 1075 standards. The non-compliant controls under the System & Communications control family include:

1. System And Communications Protection Policy And Procedures (SC-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
2. Information Remnance (SC-4): EDD does not prevent unauthorized and unintended on formation transfer via shared system resources.
3. Information Integrity (SC-8): EDD's information system does not protect the integrity of transmitted information.
4. Transmission Confidentiality (SC-9): EDD's information system does not protect the confidentiality of transmitted information.
5. Network Disconnect Control (SC-10): EDD's system does not terminate a network connection at the end of a session or after 15 minutes of inactivity.

RISK: Strong system and communications protection policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without system and communications protection policy and procedures, EDD does not have a standardized approach to formally document and implement system and communications protection policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

RECOMMENDATION: EDD Management should:

1. SC-1 System And Communications Protection Policy And Procedures: Develop system and communications protection policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the Agency. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required.
2. Information Remnance (SC-4): Configure and document procedures for the information system regarding the use of encryption for data transmitted over an unsecured network. EDD management should ensure that it is FIPS 140-2 compliant.

3. Information Integrity (SC-8): EDD's information system shall institute a procedure to securely verify that all transmissions have integrity checks, that is, the recipient is assured that what they receive is what was sent.
4. Transmission Confidentiality (SC-9): EDD's information system shall protect the confidentiality of transmitted information, by having all transmissions encrypted with an approved protocol or installing another acceptable system, such as total fiber optics within an enclosed and protected area.
5. Network Disconnect Control (SC-10): EDD's system settings should terminate a network connection at the end of a session or after 15 minutes of inactivity.

AGENCY REPONSE: The EDD is in compliance with SC-1, SC-4, SC-8, SC-9 and SC-10. The EDD Information Security Policy protects EDD information, communications, networks, systems, applications, equipment, facilities, and other information assets and sets the information security standards as summarized below:

1. Information Security Policy
2. Organization Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Automated Systems Development and Maintenance
9. Business Continuity Planning Management
10. Compliance

The EDD Employee Access Control Policy further protects the network by providing system disconnect controls.

Policy Statement:
The EDD Employee Access Control Policy ensures consistent protection of data integrity and information security of all programs, systems, and business applications within the EDD. Before individuals are granted access rights, they must complete their information security training, locally required training, and sign the appropriate non-disclosure agreements. Each automated information session must start with the person establishing their identity and authorizations (unique personal identifier and password).

(See Attachments 8 and 17)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technology Specific Findings

A representative sample of platforms (see completed SCSEMs for the list of names) was tested to drive the findings listed in this section. Although the findings were identified on the specific platforms tested, corrective actions recommended for each technology in this report should be tested and implemented on ALL platforms (with the same technology) that store, transmit, or process FTI.

Identification & Authentication – AIX

H.16 FINDING: According to the on-site evaluation performed password control at the system level is inadequate.

DISCUSSION: Discussion with system administrators revealed that the system level password controls are inadequate.

1. System level passwords are not set to have aging.
2. System level passwords are not required to meet standards of password length.
3. System level passwords are able to reset to any previous password.
4. System level individuals do not receive a password expiring notice.
5. System level passwords are not checked against standard vulnerable passwords.

RISK: The risk in having weak passwords, particularly at the system level, is that any individual with access to the system at the administrative level should have little difficulty in gaining control of the system with its FTI data in a minimum of time. Although it is the case that physical access to administrative terminals is restricted by location it is possible for an individual to gain access via the network. Even if the discussion concerns only individuals with system administrative rights it is relatively easy for such a administrator to use the identity of another system administrator to compromise the system and its FTI.

RECOMMENDATION: EDD Unix administrators should ensure that:

1. Passwords shall be changed every 90 days, at a minimum, for standard user accounts to reduce the risk of compromise through guessing, password cracking or other attack & penetration methods. Passwords shall be changed every 60 days, at a minimum, for privileged user accounts to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods. Set maxage=90
2. Passwords shall be a minimum length of 8 characters in a combination of alpha and numeric or special characters. Set minlen=8, minalpha=8
3. Users shall be prohibited from using their last six passwords to deter reuse of the same password. Set histexpir=6
4. The information system shall routinely prompt users to change their passwords within 5-14 days before such password expires. Set pwdwarntime=14
5. Use of dictionary words, popular phrases, or obvious combinations of letters and numbers in passwords shall be prohibited when possible.

Obvious combinations of letters and numbers include first names, last names, initials, pet names, user accounts spelled backwards, repeating characters, consecutive numbers, consecutive letters, and other predictable combinations and permutations. Use a password checker on the password file.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.17 **FINDING**: According to the on-site evaluation performed the information system protects audit information and audit tools from unauthorized access, modification, and deletion.

DISCUSSION: Access to the audit information is available to root. For operational requirements that access to su root lies only with system administrators and data base administrators.

RISK: The risk of having access to audit data not held extremely close is that audit data can then be manipulated by unauthorized individuals. A compromise of the audit records:

1. makes reliance on audit records impossible
2. unreliable audit records make the identification of the cause of disruptive or unauthorized acts on the system extremely difficult
3. unreliable audit records make the tracking of FTI exposure unreliable
4. an unreliable audit record makes findings inadmissible as evidence in a prosecution or adverse personnel action.

RECOMMENDATION: None. All requirements are met.

Access Control – AIX

H.18 **FINDING**: According to the on-site evaluation performed the organization does not review information system accounts to ensure that existing accounts are being controlled properly as required by IRS Publication 1075.

DISCUSSION: The UNIX administrators stated that they do not review accounts on a routine basis. It was their feeling that they knew everyone with access to their system and that such a periodic review was unnecessary.

RISK: The risk associated with a failure to review system accounts lies in the real possibility of having an individual account which should no longer have access remain active. If this account has no authorized user it could be exploited by another individual to access system resources. Activity on such an account would likely go unnoticed since the account had been authorized. Leaving accounts on any system when they are no longer authorized exposes the system and the FTI data it contains.

RECOMMENDATION: EDD management should establish a written policy which requires periodic and systematic review of all accounts on any system which manipulates, stores, or has any access to FTI material system. EDD management must have required audits performed and documented. Audit logs should be sent to a logger file (e.g. logger.edd.ca.gov), reviewed and rotated on a regular basis. All logs passed to the logger should be parsed on a routine basis via cron with a program such as logcheck.sh. The logs should include:

1. authlog
2. cronlog
3. daemonlog
4. lprlog
5. kernlog
6. newslog
7. sudo.log
8. tcpwrap.log
9. syslog.log
10. mail.log
11. ssh.log

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.19 **FINDING**: According to the on-site evaluation performed the agency does not adhere to the principle of least privilege when creating user accounts. EDD has not controlled the issuance of authorizations using the least privilege tenants.

DISCUSSION: The principle of least privilege is used when creating users and groups on the UNIX system. Industry standard practice is to create user ID and group ID permissions using UNIX Access Control Lists (ACLs) in AIX. EDD fails to exercise least privilege in that all accounts at the system level are assigned access to all administrative rights. Assignment of users to the application program is administered by the application program.

RISK: The risk in not checking the authorization levels for users and assigning users all equally powerful rights is that individuals will have control over the system that exceeds their level of responsibility. This increases the probability of deliberate or inadvertent introduction of harmful procedures that can damage the system and expose FTI material. Control of all user accounts should be controlled by the system administrator.

RECOMMENDATION: EDD management should create a written policy stating the levels of system access to be granted to individual roles. The system administrators should create procedures to implement that policy. The system administrators should control all user access to the system and to any applications residing on the system. System administrators should coordinate with the application owners and the data owners to establish procedures for granting access to the application and FTI data.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the

Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.20 **FINDING:** According to the on-site evaluation performed the system does not display an appropriate warning banner before authentication.

DISCUSSION: The system is not configured to display a logon banner containing any information about the sensitivity, confidentiality, or the consequences for misuse of the system.

RISK: A warning banner serves two purposes. First, it is a tool to warn a would-be attacker that they are attempting to access a government resource and their actions will be monitored. Second, it is a tool to help aid prosecution of attackers that have compromised a system. If the banner doesn't cover these two areas an attacker could potentially avoid prosecution by claiming they weren't aware they were accessing a government computer system.

RECOMMENDATION: The EDD Unix administrator should set a warning banner for the following system directories: /etc/motd, /etc/issue, and /etc/security/login.cfg. The banner should identify that the system is for authorized users only, user activity is monitored, and that improper use of the system will result in Federal/State criminal and/or civil penalties. The warning banner language should speak to both authorized and unauthorized users, which would cover malicious insider users as well as attackers from outside. The warning banner shown before a successful connection to all network devices should be similar to the following:

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.

If the device can only support a short banner, the contents of the banner should be:

WARNING! US GOVERNMENT SYSTEM. Unauthorized access prohibited by Public Law 99-474 "The Computer Fraud and Abuse Act of 1986". Use of this

system constitutes CONSENT TO MONITORING AT ALL TIMES and is not subject to ANY expectation of privacy.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Auditing – AIX

H.21 **FINDING**: According to the on-site evaluation performed the UNIX audit logs are not capturing events as required by IRS Publication 1075 standards.

DISCUSSION: Discussion with the system chief administrator revealed that at the system level only login and logout records are kept in the system audit trail. The system administrator explained that the system is accessed by only a few system administrators in any direct fashion. The chief system administrator does review the log information available on a daily basis, checking for unusual activities on the part of the staff. Auditing of the use of the application programs maintained on the system has been the responsibility of the application program staff. The system administrator stated that since there is no charge-back for system usage tracking of the application users was deemed unnecessary.

RISK: This lack of detailed audit logs leaves the system incapable of tracking the use of the system. The system administrative staff has no audit trail to uncover what process may have caused a malfunction on the system and no true way, at the system level, of knowing who has accessed FTI data.

RECOMMENDATION: EDD management should require the UNIX administrators to establish audit trails to capture activities for all users of the system, including system administrators. The audit trail must be expanded to:

1. Capture all successful login and logoff attempts.
2. Capture all unsuccessful login and authorization attempts.
3. Capture all identification and authentication attempts.

4. Capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users).
5. Capture all actions, connections and requests performed by privileged functions.
6. Capture all changes to logical access control authorities (e.g., rights, permissions).
7. Capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
8. Capture the creation, modification and deletion of user accounts and group accounts.
9. Capture the creation, modification and deletion of user account and group account privileges.
10. Capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event.
11. Capture system startup and shutdown functions.
12. Capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s).
13. Capture the enabling or disabling of audit report generation services.
14. Capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.22 **FINDING**: According to the on-site evaluation performed the audit records are not maintained for a period required by IRS Publication 1075.

DISCUSSION: The UNIX system logs are rotated over a 30 day period. The system utilizes a cron job at week's end to move data to alternate storage and clear the system log storage area. Over the history of the AIX system this has been adequate storage of audit material.

RISK: While the current practice has been adequate it is possible that a longer retention period for system logs may be advisable. A flaw in the system might not cause an interruption in operations for several months. If that should be the case EDD has no ability to review the system logs. This will prevent an adequate correction of a fault in the system or system security.

RECOMMENDATION: EDD management should direct UNIX system administrators to maintain audit logs for a period of six (6) years. To conserve media, logs should be taken from the monthly log, already gathered, and consolidated on media removed from the system. This media should be stored in an alternate location, off-line. Policy should then fix a retention period for these audit logs. The IRS Publication 1075 specifies a retention period of six (6) years. See Section 5.6.2, Audit and Accountability, on page 22.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.23 **FINDING**: According to the on-site evaluation performed local or syslog server has enough space to capture and retain the logs generated by the system.

DISCUSSION: The procedure for capturing audit logs relies on a cron job to round robin the log for 30 days. The items in the logs are time stamped for use in log generation. Discussions with the system administrators revealed that log space has never been overrun.

RISK: The risk of having insufficient log space is that logs will either overwrite previous log entries or fail to record current activity. In either event vital data in the log audit record is lost making it impossible to reconstruct the causes of system failure or compromise. There will be insufficient data upon which to build corrective actions. It would then be possible for a perpetrator to have entered the system and seize or alter FTI data without an ability of system or investigative personnel to reconstruct the activity to asses the exposure, to identify the perpetrator, and to successfully have an untainted trail of evidence to use in prosecution of offenders.

RECOMMENDATION: None. All requirements have been met.

H.24 **FINDING**: According to the on-site evaluation performed EDD has no written procedure for audit review.

DISCUSSION: Having an informal, daily review of the system audit raises the possibility that either new personnel will be unaware of the procedure or current personnel will ignore what is only a local tradition without the support of a documented procedure. Although the interview revealed that only a select few individuals have authorized access to the UNIX system their activities need be audited and that audit trail reviewed.

RISK: The risk to FTI data and to the UNIX system is that an unauthorized user or disgruntled employee could commit malicious acts on the system compromising FTI data and such activity would be untraceable under the current audit conditions. Having no written policy requiring audit review renders no one responsible or liable for the audit review.

RECOMMENDATION: EDD management should develop a written policy requiring daily review of its UNIX system's audit.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the

Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Configuration Management – AIX

H.25 FINDING: According to the on-site evaluation performed the system does not use securetcpip.

DISCUSSION: Examination of the UNIX system and discussions with the UNIX system administrator disclosed that securetcpip is not installed and operational on the system.

RISK: Without securetcpip several communication protocols have settings that allow the running of untrusted commands and daemons. These commands may be activated by an application program or other user procedure and transmit FTI data to unauthorized procedures or users.

RECOMMENDATION: The EDD UNIX administrator should use the securetcpip command to provide enhanced security for the network. This command performs the following:

Runs the tcbck -a command, which disables the nontrusted commands and daemons: rcp, rlogin, rlogind, rsh, rshd, tftp, and tftpd. The disabled commands and daemons are not deleted; instead, they are changed to mode 0000. A particular command or daemon can be enabled by re-establishing a valid mode.

Adds a TCP/IP security stanza to the /etc/security/config file. The stanza is in the following format:

```
tcpip:
  netrc = ftp,rexec     /* functions disabling netrc */
```

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

System & Communications Protection – AIX

H.26 **FINDING**: According to the on-site evaluation performed the UNIX system does not terminate a network connection after 15 minutes of inactivity.

DISCUSSION: Examination of system configuration files and discussion with UNIX administrators disclosed that there is no session termination after a period of inactivity at the system level. The rationale put forth is that the facility is a closed facility and there are only a very limited number of individuals at the facility with authorized access to the UNIX system. It was therefore the opinion of the UNIX administrator that termination for inactivity was unwarranted.

RISK: The risk of having no termination after a period of 15 minutes of inactivity, is that the session can be pirated by another user who will then have unauthorized access to system resources including FTI data.

RECOMMENDATION: The EDD UNIX administrator should implement session termination for all sessions inactive for a period longer than 15 minutes.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

System Reviewed: DATA31 – Windows 2003 server

Identification & Authentication – Windows 2003

H.27 **FINDING**: According to the on-site evaluation performed password composition does not meet IRS Publication 1075 requirements.

DISCUSSION: Analysis of the Local Security Policy setting shows that:

1. Password length is not required to be between 8 and 128 characters, but fewer numbers of characters.
2. Passwords do not meet complexity requirement. The value for "Passwords Must Meet Complexity Requirements" is set to Disabled in the local security policy.

RISK: Without proper password length or complexity rules enforced, it is easier for an adversary to crack user passwords (especially for privileged accounts, such as System Administrators [SA] users), resulting in unauthorized system access and potential unauthorized disclosure of FTI data.

RECOMMENDATION: The following recommendations are suggested for the Windows server:

1. Open Local Security Policy
2. Ensure password length is set to 8 characters
3. Ensure password complexity setting is Enabled

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.28 **FINDING**: According to the on-site evaluation performed password aging settings do not meet IRS Publication 1075 requirements.

DISCUSSION: Analysis of the system Local Security Policy settings shows that the password aging requirement is not enforced. IRS Publication 1075 requires a minimum age of 15 days for all passwords. Windows password aging parameter is set to "0" days, which allows a user to change their password at any time, without waiting for the required 15 days. This means that, once a user changes their password, the user is not prevented from changing their password back to previous values.

A review of the system shows that there are only two administrators' accounts on the system and no user accounts. Therefore, the risk of this item is reduced, so long as normal user accounts are not added to the system.

RISK: Not enforcing password aging can allows a user to continue to use their old passwords, which may defeat the purpose of password aging.

RECOMMENDATION: The following recommendations are suggested for the Windows server:

1. Open the Local Security Policy.
2. Move to Password Policy.
3. Set the value for the "Minimum password age" to 15 days.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Access Control – Windows 2003 Server

H.29 FINDING: According to the on-site evaluation performed vulnerable or unnecessary network services are enabled and running.

DISCUSSION: Analysis of the list of services on the server shows that vulnerable or unnecessary network services are enabled and running. For example, the following services are found to be running on the systems analyzed:

1. SNMP
2. Alerter
3. Remote Registry Service

Agency management indicated that SNMP is required for management of the system. The test revealed that Telnet, FTP, and Messenger are disabled.

RISK: Running unnecessary network services increases the risk of unauthorized access to the system and FTI. Enabling vulnerable or unnecessary services provides avenues for an attacker to compromise a system. The more services running on a computer, the more entry points you make available to unauthorized users. A service is a potential entry point because it processes client requests. To help reduce this risk, management should disable unnecessary system services.

SNMP service generates trap messages that are sent to a trap destination. A malicious user could utilize these services to perform a task that creates security vulnerability. Using insecure protocols such as SNMP provides eavesdropping capability for an adversary.

RECOMMENDATION: Institute a policy that mandates only required services necessary for the system to function are enabled. Further, implement SNMPv2 to replace SNMP.

Agency management should disable all running services that do not have a genuine business requirement for their existence on the Windows systems.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.30 **FINDING**: According to the on-site evaluation performed the system allows anonymous enumeration of SAM accounts and shares.

DISCUSSION: Analysis of the Local Security Policy shows that the system permits anonymous access to SAM accounts and shares – anonymous network access to lookup account names, user groups, and file shares is not restricted. Providing NULL session connections allows an attacker or malicious user to access system resources without authentication.

RISK: Permitting anonymous access to SAM accounts and shares (NULL session connections) allows an attacker or malicious user to access confidential login credentials, list account names and enumerate share names. This information can later be used to launch other attacks. For example, a malicious individual could use this information to foot print a system. Foot printing is the process of gathering information about a system before an unauthorized user attempts to hack the computer and access FTI.

RECOMMENDATION: Using Microsoft Windows Local Security Policy tool:

Set the value for the Security Option, "Network access: Do not allow anonymous enumeration of SAM accounts and shares" to "Enabled"

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.31 **FINDING**: According to the on-site evaluation performed encryption is not being used when accessing Windows ("remote desktop") from other systems in the network.

DISCUSSION: A review of the registry setting shows that encryption is not being used when remotely accessing Windows operating system from other systems within or outside the network. There is no value set for the required registry key:

HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Conferencing\
Value Name: NoRDS

During the testing, EDD management indicated that encryption is not required for all communications within EDD's internal network.

RISK: Failure to use encryption to protect the confidentiality of remote access sessions can result in data interception by an unauthorized third-party eavesdropping on a network connection between EDD's system and an authorized user.

RECOMMENDATION: To ensure that encryption is being used when accessing Windows from other systems, create the registry key below and set the value to 1:

HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Conferencing\
Value Name: NoRDS

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.32 FINDING: According to the on-site evaluation performed Windows Messenger Internet Access is enabled.

DISCUSSION: A review of the registry setting shows that Windows Messenger Internet access is enabled. In addition, users can launch Windows Messenger (MSN Messenger, .NET Messenger). There is no Messenger sub key.

A review of the system shows that there are only two administrator accounts on the system and no user accounts. Therefore, the risk of this item is reduced, so long as normal user accounts are not added to the system.

RISK: Enabling Windows Messenger Internet Access could result in potential confidential FTI data or data files being transmitted to other systems.

RECOMMENDATION: Although normal user accounts are not present in the system currently, Windows messenger needs to be disabled in case users are created on the local system.

Create the registry keys below and set the value to 1:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Messenger\Client\{9b017612-c9f1-11d2-8d9f-0000f875c541}

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Messenger\Client
Value Name: PreventRun

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.33 **FINDING**: According to the on-site evaluation performed there are irrelevant files and registry entries in the system.

DISCUSSION: A review of the registry shows that there are no entries for the keys searched. Further, a listing of the "dllcache" directory does not show irrelevant files. In addition, there is no "os2" directory in the file system. However, the keys "Optional" and "Posix" exist.

magnetic tape to the IT Cannery site where it is loaded to the tape library. The tape run is scheduled and brings the information on to the mainframe. The courier returns the tape to the TAS office where it is picked up by a Tax Support Division employee. FTB is contacted, picks up and returns the tape to California Franchise Tax Board (CA FTB). Tapes are processed along mainframe. Data is not kept on mainframe. After 300 days, any backup tapes are scratched.

RECOMMENDATION: None, all requirements have been met.

A.3 **FINDING:** EDD has an adequate system for controlling FTI.

DISCUSSION: EDD has a permanent system of standardized records, which documents FTI that has been transferred to EDD examination reports and case files. In using FTI, EDD tax examiners may transcribe FTI into their examination reports. EDD tracks all their case files that have FTI. EDD employees are required to label and track commingled FTI by using the FACD online log from the date of the request to the date of destruction.

RECOMMENDATION: None, all requirements have been met.

B. MAINTAINING A SECURE PLACE FOR STORAGE OF TAX RETURNS AND RETURN INFORMATION

Requirement: 26 USC §6103(p)(4)(B) requires that a secure place or area be maintained where federal tax information is stored. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 4, pages 9 through 15.

B.1 FINDING: Federal tax information is properly stored and protected in the EDD headquarters building at 722 Capitol Mall, Sacramento, CA.

DISCUSSION: Entrances to the 2 main entrances are secure. Anyone without a card key must enter through the main entrance. Building security guards verify identification. A visitor's sticker badge is issued after information in a visitor's log book has been completed. All special visitors receive numbered badges. Visitors are directed to the building manager's office where a contact is called. The contact comes downstairs to the lobby and escorts the visitor to the area being visited. The visitor's badge is returned to the guard desk after completion of the visit. Card keys with photo identification are used by CA EDD employees are used for areas not open to the public. The entrance doors are locked after hours. The building is EDD owned and is not shared with any other state agencies. Janitorial services are performed during normal office hours. The Tax Information Security Officer receives FTI from the IRS Oakland Disclosure Office and the Fresno RAIVS Unit in response to individual requests from EDD employees. Until distributed to EDD employees, the FTI is maintained in a locked cabinet with a combination lock. Only authorized employees have the combination. Entrance to the Tax Information Security Officer's area is by card key only.

RECOMMENDATION: None, all requirements have been met.

B.2 FINDING: Federal tax information is properly stored and protected in the Field Audit and Compliance Office at 3321 Power Inn Road, Sacramento, CA.

DISCUSSION: Minimum Protection Standards (MPS) were met at the field office site. EDD shares the building with several other state agencies. Property management provides security guards on a 24-hour basis. The public does not have access to EDD space. All doors have combination locks. All EDD employees are aware of and instructed to abide by the *EDD Clean Desk Policy* and store confidential records in locked containers, file cabinets, and/or desk drawers during non-work hours. The

office manager or their designated backup is responsible for inspecting the area, locking all doors, and activating the alarm at the end of each workday. Closed audit files containing FTI are kept in the locked file room, in non-locking cabinets, commingled and labeled as FTI appropriately. Active working cases are kept at the employee's desk and are required to be locked in desk drawers during non-work hours. Pursuant to CA EDD FAC Notice No.04-01 (4-09-2004), all hard copy case files and associated diskettes must be clearly labeled to indicate that they contain FTI. The marking of the case file will take place when the FTI is received and placed in the file, and will be done by stamping or writing "contains FTI" on the outside of the case folder. The marking of the file diskette will be done the same way and will take place when case information has been saved.

RECOMMENDATION: None, all requirements have been met.

B.3 FINDING: Federal tax information is properly stored and protected in the Investigations Division office at 2411 Alhambra Blvd., Sacramento, CA.

DISCUSSION: Minimum Protection Standards (MPS) were met at the Investigations office site. The public does not have access to Investigations Division space. A visitors log is filled out at the reception area and visitors are escorted into the office. All doors have combination locks. All EDD Investigation employees are aware of and instructed to abide by the *EDD Clean Desk Policy* and store confidential records in locked containers, file cabinets, and/or desk drawers during non-work hours. The manager or his designated backup is responsible for inspecting the area, locking all doors, and activating the alarm at the end of each workday. Closed investigation files containing FTI are kept in the locked file room, in non-locking cabinets, commingled and labeled as FTI appropriately. Active working cases are kept at the employee's desk and are required to be locked in desk drawers during non-work hours. I reviewed 5 cases and although cases were marked FTI, the tax returns were 3rd party information supplied by the person being investigated, thus not FTI. This information is allowed in the case file as long as it is properly marked or stamped as being received from the person being investigated.

RECOMMENDATION: None, all requirements have been met.

B.4 FINDING: Federal tax information is properly stored and protected in the DTS Cannery Campus (Computing Center) at 1651 Alhambra Blvd., Sacramento, CA.

DISCUSSION: The DTS Cannery Campus processes information for various state agencies, in addition to CA EDD. The DTS Cannery maintains a browser based application, Intranet Field Audit Compliance System (IFACS) for CA EDD. The physical security for the entrance to and within the facility meets IRS standards. State of California employees occupy the facility 24 hours per day, 7 days a week. Contracted guard service is in place at the entrance at all times. Entrance to the facility is strictly controlled. All doors are monitored. Non-Data Center visitors who have a demonstrated need for frequent and regular Data Center access must go through a clearance process before being issued a Data Center cardkey. All other visitors are identified, authenticated and given a badge prior to admission through an automated access control visitor system. They must be escorted at all times by a Data Center employee, who meets them at the entrance, which is at the guard area. After admission to the work area, there is a holding area for additional verification prior to entry to the main work area. The entire building perimeter and all interior areas are continually monitored by the contracted guard service via closed circuit TV cameras. The guard service also conducts roving patrols and walkthroughs of the work areas and outside perimeter. There is an alarm system monitored 24 hours per day. Janitorial services are provided during the day.

Entrance to the computer room and tape library is further restricted via the cardkey access control system. The authorized employee's cardkey is coded to restrict access solely to areas within the Data Center where access is required. The computer room is not well inside the building – none of the walls face outside, nor are there any windows. Standard fire safety provisions for computer rooms are in place, including sprinklers and Halon for fire suppression.

RECOMMENDATION: None, all requirements have been met.

B.5 FINDING: All FTI transported is not maintained in a secure manner.

DISCUSSION: When receiving completed requests for information from the RAIVS unit, the Tax Information Security Office confirms the authorized user from their list. If there is no information sent by the RAIVS Unit, this information is sent to the requester in a regular envelope. A return copy of the information is also sent back to the RAIVS Unit in a regular envelope. If there is return

information received by the Tax Information Security Office, that information is sent to the requester in a double sealed envelope.

RECOMMENDATION: All FTI transported through the mail or courier/messenger service must be double sealed, that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designated official or delegate is authorized to open it. All shipments of FTI must be documented with a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged.

AGENCY RESPONSE: The Employment Development Department (EDD) is in compliance with Internal Revenue Service's (IRS) recommendation. The EDD's Administrative Circular No. 05-02B issued on May 3, 2005 provides packaging requirements for shipment of confidential information. It states that all packages containing FTI must be doubled-packed with a sealed, inner envelope/container and a sealed outer envelope or reinforced cardboard box. The Administrative Circular attachments also states logging and monitoring of packages containing. This policy remains in force.

IRS : Agency response accepted

B.6 FINDING: Under Federal tax regulations § 301.6103(p)(2)(B)-1, EDD receives FTI from CA FTB.

DISCUSSION: The Tax Information Security Officer receives the tape from a CA FTB employee who hand delivers the magnetic tape. The tape is taken down to the Tax Accounting system and brought across the street to the "Solar" building where a work order is created by a Tax Accounting System (TAS) analyst. A courier transports the magnetic tape to the IT Cannery site where it is loaded to the tape library. The tape run is scheduled and brings the information on to the mainframe. The courier returns the tape to the TAS office where it is picked up by a Tax Support Division employee. FTB is contacted, picks up and returns the tape to California Franchise Tax Board (CA FTB). Through out the process, the tape was not properly labeled as FTI and afforded the double sealed barrier of protection for FTI being transported as required by publication 1075.

RECOMMENDATION: None. EDD no longer receives magnetic tapes from CA FTB. CA FTB has notified CA EDD that they will no longer be supplying 1099-MISC information by magnetic tape. CA FTB will only supply the information by electronic transfer means should CA EDD wish to continue receiving it from them. EDD is now testing SDT and will secure 1099-MISC

and LEVY information directly through the Internal Revenue Service. However, should CA EDD receive any other FTI in the future from CA FTB, procedures must be in place to properly log, protect and identify the received FTI information.

AGENCY RESPONSE: If the EDD receives any other FTI in the future from the Franchise Tax Board, procedures will be in place to properly log, protect and identify the FTI information.

IRS: Agency response accepted

B.7 FINDING: There is no warning banner reflected on the computer screen before an employee signs on to the Intranet Field Audit Compliance System (IFACS) system banner reflected on the computer screen before an employee signs on to the IFACS system.

DISCUSSION: Based upon the review at the 3321 Power Inn Rd. office, there is no warning banner present on CA EDD's IFACS system.

RECOMMENDATION: As stipulated by OMB 1545-0962, a warning banner advising of safeguarding requirements should be displayed on the screen of any computer accessing a system that stores, processes, or transits FTI. Consult your legal counsel to confirm /modify the appropriate wording of the warning banner. The system must write the full banner to the screen and pause to permit the user to read the banner before allowing them to proceed. As approved by the Department of Justice:

Warning! BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM YOU ARE CONSENTING TO SYSYTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

OR:

This is a FTI specific warning banner:

WARNING

This system may contain government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject to the

individual to criminal and civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (The Taxpayer Browsing Protection Act) and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING

Another acceptable warning banner that includes the four elements discussed would be adequate: They are:

1. Government System
2. Authorized Usage
3. Monitoring
4. Subject to Federal/state criminal or civil penalties

CA EDD can use any of the above, or construct their own warning banner that includes the four items above.

AGENCY RESPONSE: The EDD is in compliance with IRS recommendation. The following warning banner was added to IFACS on June 20, 2008.

WARNING

By accessing and using this government computer system, you are consenting to system monitoring for law encfrcement and other purposes. Unauthorized use of, or access to, this computer system may subject you to criminal prosecution and penalties.

Prior to logging on IFACS, the above warning banner appears and pauses to permit the user to read the banner. Before allowing the user to log on the user must select OK

IRS: Agency response accepted:.

C. LIMITING ACCESS TO TAX DATA TO EMPOYEES OF THE AGENCY WHO HAVE A NEED-TO-KNOW AND WHO ARE AUTHORIZED TO HAVE ACCESS

Requirement: 26 USC §6103(p)(4)(C) requires that access to federal tax information be restricted to persons whose duties require access and to who disclosure may be made under provisions of law. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 5, pages 17 through 19.

C.1 FINDING: Access to FTI and areas containing FTI are restricted to those personnel with a "need to know" and who are authorized by law to have access to the FTI data.

DISCUSSION: Managers designate employees authorized to receive Federal tax information and ensure that those employees have a "need to know". When an employee EDD employee leaves the agency, the manager notifies the Tax Information Security Officer. EDD has written procedures for disclosing information to others than the data subject. Those procedures require a written consent to be presented to the Department within 30 days of the date the consent was signed. The only employees who have access to FTI requested on an individual basis are the Tax Information Security Officer and her assistant. When the FTI is received, it is logged and forwarded to the person who made the request. The Chief, Audit Section, Field Audit and Compliance Division, receives examination reports. Only a Tax Administrator and Program Technical have access to these reports before distribution to the appropriate field offices. Only designated employees my process these reports in field offices. Logs are maintained on who has control of these examination reports.

RECOMMENDATION: None, all requirements have been met.

C.2 FINDING: Contract cleaning crews and maintenance crews do not have access to FTI.

DISCUSSION: Based upon discussions held at several offices, it was determined that the maintenance and cleaning crews have access to the office areas during the day and possibly at night in some locations. However, these crews do not have access areas where FTI is stored without a BSCE employee being present. At DOIT, cleaning personnel are not allowed in the computer room unless there is at least one DOIT employee present and under no circumstances may any cleaning personnel be authorized to open an outside door to allow entry to an individual.

RECOMMENDATION: None, all requirements have been met.

C.3 **FINDING:** CA EDD restricts access to the FTI received from CA FTB.

DISCUSSION: CA EDD has approximately 400 IFACS Users. Approximately 150-200 IFACS Users have access to the screens that house the 1099-MISC data supplied by CA FTB. Auditing programs are in place that track the access to the IFACS system.

RECOMMENDATION: None, all requirements have been met.

D. PROVIDING OTHER SAFEGUARDS DETERMINED TO BE NECESSARY

Requirement: 26 USC §6103(p)(4)(D) requires that other safeguard measures be provided that the Secretary of the Treasury determines to be appropriate to protect confidentiality of federal tax return information. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 6, pages 25 and 26.

D.1 **FINDING:** EDD has computerized training and awareness programs for their employees. All affected employees have access and opportunity to review a computerized security awareness presentation on computers at their work stations.

DISCUSSION: EDD uses computer based training (CBT). Each employee is required to sign a Tax Branch Confidentiality statement annually (DE 7410). The EDD also has Information Practices Handbook which addresses confidentiality and disclosure concerns. Employees are advised of criminal penalties for unauthorized access as well as unauthorized access as well as unauthorized disclosure of information. The Tax Disclosure Office now requires written (e-mail) confirmation from each of the four Tax Branch Division Chiefs once all employees have completed the annual Tax Branch I *Confidential Information and Security Awareness* computer based training module. This module includes a UNAX section and specific references to the administrative and legal consequences for unauthorized access, use and disclosure of FTI.

RECOMMENDATION: None, all requirements have been met.

D.2 **FINDING:** CA EDD's awareness program has been expanded.

DISCUSSION: The Tax Disclosure Office has issued a series of periodic e-mails to CA EDD staff reminding them of the administrative and legal consequences for unauthorized access, use and disclosure of FTI.

RECOMMENDATION: None, all requirements have been met.

E. SUBMISSION OF REQUIRED SAFEGUARD REPORTS

Requirement: 26 USC §6103(p)(4)(e) requires that reports be furnished to the Secretary of the Treasury, which describes the procedures established and utilized to ensure the confidentiality of tax data received from the IRS. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 7.

E.1 **FINDING:** A Safeguard Procedure Report (SPR) was submitted as required and is on file.

DISCUSSION: EDD's SPR is dated January 1996. The new Publication 1075 outlines that an SPR is now due every six years or when significant changes occur in the agency. The Safeguards office will notify EDD when to file their updated SPR within the next year.

RECOMMENDATION: None, all requirements have been met. Upon notification by the Safeguards Office, a new SPR must be submitted with the Office of Safeguards.

E.2 **FINDING:** The Safeguard Activity Report (SAR) has been submitted as required and is on file.

DISCUSSION: The latest SAR is dated March 23, 2007, received on April 3, 2007 and accepted on May 4, 2007. Issues identified with shredding and 45 day contract notification was discussed and resolved with Julia Reasoner and Ike Grisby.

RECOMMENDATION: None, all requirements have been met.

F. DISPOSAL OF RETURNS AND RETURN INFORMATION UPON COMPLETION OF USE

Requirement: 26 USC §6103(p)(4)(f) requires agencies to return tax information to the IRS, make the information "undisclosable", or, in some instances, retain the information and safeguard it. Refer to Publication 1075, Tax Information Guidelines for Federal, State and Local Agencies, Section 8, pages 31 and 32

F.1 **FINDING:** Disposal of federal tax information at 3321 Power Inn Road meets appropriate standards.

DISCUSSION: The Field Audit and Compliance Division office has 2 sixty-four gallon Plastopan security bins. Review of 6 case files found no FTI present. All FTI is put into these shredding bins after use. Datashred Inc. contacts the office comes in and takes out the 2 shredding bins to their mobile shredding vehicle and shreds the material on-site. The office Tax Adminstrator witnesses the shredding from the shredding bins.

RECOMMENDATION: None, all requirements have been met.

F.2 **FINDING:** EDD/Datashred, Inc. contract #M660711 does not contain the appropriate safeguard language.

DISCUSSION: I reviewed the latest contract of Datashred Inc. (effective 5/1/2006 – 03/31/2008). The contract in Section II. E. Confidentiality of Data contains an outdated reference to Exhibit 5 in Publication 1075.

RECOMMENDATION: The current EDD/Datashred contract and all future contracts must include Publication 1075's, Exhibit 7 Contract Language For General Services which outlines the criminal and civil penalties for unlawful disclosure of Federal Tax Information and inspection of the offices by the IRS and the agency to verify the performance of work under this contract.

AGENCY RESPONSE: The EDD is in compliance with IRS recommendation. Publication 1075's Exhibit 7 is included in the current EDD/Datashed contract #M869121 (effective April1, 2008-March 31, 2009)

IRS: Agency response accepted

F.3 **FINDING:** EDD's Confidentiality Agreement that is attached to EDD/Datashred Inc. contract #M660711 and Department of Technology Services does not contain the appropriate safeguard language.

DISCUSSION: Agencies are encouraged to use specific safeguard language in their contractual agreements and confidentiality agreements to avoid ambivalence, ambiguity and advising all employees, contractors of the provisions of IRC §7213, 7213A and 7431.

RECOMMENDATION: All EDD current and future confidentiality agreements must include the provisions of IRC 7213, 7213A and 7431. Please refer to the language outlined in Publication 1075's Exhibit 10, IRC Sec. 7213 and 7213AUnauthorized Disclosure of Information and Exhibit 5, IRC 7431 Civil Damages for Unauthorized Disclosure of Returns and return information.

AGENCY RESPONSE: As of January 2008, all EDD confidentiality agreements involving FTI include the provisions of Internal Revenue Code 7213, 7213A, and 7431.

IRS: Agency response accepted.

G. NEED AND USE

Requirement: Policy Statement P-1-35 quotes that "Tax information provided by the IRS to State tax authorities will be restricted to the authorities' justified needs and uses of such information." Other agencies must use the information only for the purpose(s) authorized by statute.

G.1 **FINDING:** Federal tax data is used by the agency in accordance with the statute.

DISCUSSION: Disclosure of return information to the agency is prescribed by statute. Tax data disclosed to the California Employment Development Department under the provision of IRC §6103(p)(2) and IRC §6103(d) is used by the agency for use in audit leads for noncompliant employers by Field Audit and Compliance Division and by the Collection Division to locate delinquent taxpayers, identify revenue sources and aid in the determination of the collectability of an account.

EDD receives Form 1099-MISC information from the IRS through the Franchise Tax Board (FTB). FTB receives the tape of Form 1099-MISC as part of the Fed/State Data Exchange program. FTB adds to the tape the combined Federal/State Form 1099-MISC media filers and creates a California universe of form 1099-MISC filers. FTB provides the universe tape to the IRS, which upon receipt of a request from EDD provides the tape to the EDD.

In calendar year 2006, 750 audits were completed from the Form 1099-MISC data resulting in a total liability change of $6,070,117.00 with an average increase in liability of $8,093 per case. Since the Form 1099-MISC data became available in 2003, the Form 1099-MISC database is reviewed for most audit cases assigned. This gives the auditor the most complete picture of the employer before the first audit appointment. The audit program feels that access to this data enhances the productivity of every case, not just only the cases generated by the Form 1099-MISC data. The use of Form 1099–MISC information is critical to EDD's audit program and for promoting compliance.

In calendar year, 2006, EDD's Collection Division (CD) searched 922 accounts and 248 matching records were located using the Form 1099-MISC information. These results revealed an average success rate of 27% in locating data on delinquent accounts.

RECOMMENDATION: None, all requirements have been met.

G.2 FINDING: Unauthorized access or inspection of FTI must be reported.

DISCUSSION: If unauthorized use or access to FTI has been identified, either by review of the mainframe-access audit trail or by visual observation, the unauthorized disclosure must be reported to the Treasury Inspector General for Tax Administration (TIGTA).

RECOMMENDATION: Upon discovery of a possible improper inspection or disclosure of FTI by a Federal employee, a State employee, or any other person, the individual making the observation or receiving information should contact the office of the appropriate TIGTA.

Field Division	States Served by Field Division	Telephone Number
San Francisco	California, Hawaii	(510) 637-2558 Or 1-800-366-4484

The mailing address is:
Treasury Inspector General for Tax Administration
P. O. Box 589, Ben Franklin Station
Washington, DC 20044-0589

AGENCY RESPONSE: The EDD will adhere to IRS recommendation. Per California Civil Code 1798.29(b), upon discovery, the Tax Information Security Office will immediately notify the Treasury Inspector General for Tax Administration of any breach, improper inspection, or disclosure of the FTI.

IRS: Agency response accepted

H. COMPUTER SECURITY

Requirement: IRS Publication 1075 requires all systems that process Federal tax data to comply with the provisions of OMB Circular A-130 and Department of Treasury Directives. Computers, which process, store, or transmit Federal tax returns or return information shall meet the minimum security requirements and standards defined in the Publication 1075.

The California Employment Development Department (EDD) currently has one system that processes, stores and transmits Federal tax information (FTI).

1. IFAX: Intranet Field Audit Compliance System (IFAX) is used as a workload management tool to assign, track, transfer, or close collections activities relating to employer accounts. The system is used by EDD Tax Branch staff to match and review files for audit purposes. FTI is loaded on to the database server from the mainframe via FTP. Users access the application remotely through the Intranet via HTTPS. The servers are located at the state Data Center at 1651 Alhambra Blvd. Sacramento, CA 95816.

Note: EDD is not currently using Tumbleweed for transfer of FTI. Although the Tumbleweed infrastructure is in place and planned to come online in January, since FTI is not currently being processed by the Tumbleweed infrastructure it is excluded from the scope of this review.

1. MOT – Findings H.1 - H.15
2. UNIX (AIX) - Findings H.16-H.26
3. Windows 2003– Findings H.27 – H.43
4. RACF – Findings H.44 – H.48

Note: The MOT findings are reported for the first time in accordance with the Publication 1075 revised in October 2007.

H. COMPUTER SECURITY

Requirement: IRS Publication 1075 requires all systems that process Federal tax data to comply with the provisions of OMB Circular A-130 and Department of Treasury Directives. Computers, which process, store, or transmit Federal tax returns or return information shall meet the minimum security requirements and standards defined in the Publication 1075.

The California Employment Development Department (EDD) currently has one system that processes, stores and transmits Federal tax information (FTI).

1. IFAX: Intranet Field Audit Compliance System (IFAX) is used as a workload management tool to assign, track, transfer, or close collections activities relating to employer accounts. The system is used by EDD Tax Branch staff to match and review files for audit purposes. FTI is loaded on to the database server from the mainframe via FTP. Users access the application remotely through the Intranet via HTTPS. The servers are located at the state Data Center at 1651 Alhambra Blvd. Sacramento, CA 95816.

Note: EDD is not currently using Tumbleweed for transfer of FTI. Although the Tumbleweed infrastructure is in place and planned to come online in January, since FTI is not currently being processed by the Tumbleweed infrastructure it is excluded from the scope of this review.

1. MOT – Findings H.1 - H.15
2. UNIX (AIX) - Findings H.16-H.26
3. Windows 2003– Findings H.27 – H.43
4. RACF – Findings H.44 – H.48

Note: The MOT findings are reported for the first time in accordance with the Publication 1075 revised in October 2007.

MOT Findings (New)

The MOT findings resulted from the evaluation of agency specific management, operational, and technical controls focusing just on FTI. The findings listed in this section are not specific to a particular technology or a system but rather address agency wide management, operational, and technical issues related to FTI.

Management Controls – Risk Assessment

H.1 **FINDING**: According to the on-site evaluation performed risk assessment controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, four Risk Assessment controls were found to not be compliant with IRS Publication 1075 standards. EDD currently does not have formal risk assessment policies and procedures in place. Processes are not in place to track to perform vulnerability assessments. The four non-compliant controls under the Risk Assessment control family include:

1. Risk Assessment Policy and Procedures (RA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
2. Risk Threat Assessment (RA-3) EDD does not evaluate and analyze the current threats and vulnerabilities in its logical or physical environment.
3. Risk Assessment Update (RA-4): EDD does not update the risk assessment at a minimum of every three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security status of the system.
4. Vulnerability Scanning (RA-5): EDD does not scan for vulnerabilities in the information system on a periodic basis or when significant new vulnerabilities potentially affecting the system are identified and reported.

RISK: Strong risk assessment policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong risk assessment policy and procedures, EDD does not have a standardized approach to formally document and implement risk assessment policy and procedures.

Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to Agency operations, Agency assets, or individuals based on the operation of the information system. Without periodic updates, evaluation and analysis of these threats and vulnerabilities may become outdated; therefore, inadequate

levels of information security may be implemented on the system, potentially allowing unauthorized access.

Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred. Failure to conduct regular vulnerability scans of the information system may expose the system to preventable risks and costs.

RECOMMENDATION: EDD Management should:

1. RA-1: Risk Assessment Policy and Procedures:
    a. Risk assessment policy and procedures need to (i) exist; (ii) should be documented; (iii) and should be disseminated to appropriate elements within EDD.
    b. Risk assessment policy and procedures (i) should be periodically reviewed by responsible parties within the agency; and (ii) should be updated, when EDD review indicates updates are required.
    c. Risk assessment policy should address the purpose and scope of the control, and should address roles, responsibilities, management commitment, coordination among agency entities, and compliance.
2. RA-3: Complete periodic assessments to evaluate and analyze current threats and vulnerabilities to ensure the security surrounding the information system is adequate to protect the system from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.
3. RA-4: EDD management should update risk assessment documentation for the information system every three years, or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact system security, to ensure that the system controls are adequate to protect the system from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.
4. RA-5: Vulnerability scanning should be conducted on systems with FTI.
    a. EDD management should scan the information system for vulnerabilities quarterly or when significant new vulnerabilities that could potentially affect the system are identified and reported.
    b. EDD management should use scanning tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact.

AGENCY REPONSE: The EDD has a documented Risk Assessment Policy and a risk assessment plan to update and complete a comprehensive risk analysis cycle at least every two years as outlined in the Enterprise Risk Management

(ERM) Framework Policy, Executive Notice No. 08-01B and Risk Assessment Policy, Executive Notice No. 03-02B.

The DTS has various standards addressing risk assessment policy and procedures. The DTS has the following standards for this area. The DTS policies "3200 Threat Management Policy," "3308 Network Server Vulnerability Scan Procedure," and "3300 Vulnerability Management Policy" address these issues.

(See Attachments 2, 3, 5, 6, and 7)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Management Controls – Planning

H.2 **FINDING**: According to the on-site evaluation performed, security planning controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, no planning controls were found to be compliant with IRS Publication 1075 standards. EDD does not formalize and conduct security planning activities. Documentation of security planning activities was not presented. The six non-compliant controls under the Planning control family include:

1. Security Planning Policy and Procedures (PL-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
2. System Security Plan (PL-2): EDD does not develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization do not review and approve the plan.
3. System Security Plan Update (PL-3): EDD does not review the security plan for the information system at least annually and revise the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
4. Rules of Behavior (PL-4): EDD does not establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization does not receive signed acknowledgement from users indicating that they have read, understand, and agree to abide by the Rules of Behavior, before authorizing access to the information system and its resident information.
5. Privacy Impact Assessment Control (PL-5): EDD does not conduct a privacy impact assessment on the information system in accordance with OMB policy.

6. Security-Related Activity Planning (PL-6): EDD does not currently plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on Agency operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

RISK: Strong security planning policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong security planning policy and procedures, the Agency does not have a standardized approach to formally document and implement security planning policy and procedures.

RECOMMENDATION: EDD Management should:

1. PL-1: Security Planning Policy and Procedures:
    a. Security planning policy and procedures (i) exist, for each control; (ii) should be documented; (iii) and should be disseminated to appropriate elements within EDD.
    b. Security planning policy and procedures (i) should be periodically reviewed by responsible parties within EDD; and (ii) are updated, when EDD review indicates updates are required.
    c. Security planning policy should address the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.
2. PL-2: System Security Plan: Develop a security plan, in accordance with NIST SP 800-18 methodology, that provides an overview of the information system and a description of the security controls planned or in place for meeting the IRS Publication 1075 security requirements. Designated agency management officials should review and approve the security plan. The review of the security plan should contain acknowledgement and acceptance from designated agency officials, i.e. (Information Security Officer, System Owner, and Service Provider).
3. PL-3: System Security Plan Update: The system security plan should be reviewed annually, by EDD management. During reviews major changes to EDD information systems and problems with security plan implementation and security control enhancements should be considered for updates to the security plan.
4. PL-4: Rules of Behavior: EDD management shall establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. EDD management should receive signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.
5. PL-5 Privacy Impact Assessment: EDD management should conduct a privacy impact assessment on the information system in accordance with OMB policy.

6. PL-6 Security-Related Activity Planning: EDD management should plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on Agency operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

AGENCY REPONSE: The EDD is in compliance with PL-1 through PL-6. The EDD Information Security Policy protects EDD information, communications, networks, systems, applications, equipment, facilities, and other information assets and sets the information security standards as summarized below:

1. Information Security Policy
2. Organization Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Automated Systems Development and Maintenance
9. Business Continuity Planning Management
10. Compliance

The EDD is in compliance with IRS' recommendation. The EDD has a mandatory computerized security awareness training program for employees which must be completed on an annual basis. The Security Awareness Training and Education is managed by EDD's Information Security Office (ISO). Upon completion of this training, each employee is required to sign a Confidentiality Statement (DE 7410) which is filed in their personnel file.

(See Attachments 8, 9, and 10)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Management Controls – System & Services Acquisition

H.3 FINDING: System & Services Acquisition controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, ten System & Services Acquisition controls were found to not be compliant with IRS Publication 1075 standards. The ten non-compliant controls under the System & Services Acquisition control family include:

1. System and Services Acquisition Policy and Procedures (SA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented

procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

2. Allocation of Resources (SA-2): EDD does not determine, document, and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system.
3. Life Cycle Support (SA-3): EDD does not manage the information system using a system development life cycle methodology that includes information security considerations.
4. Acquisitions (SA-4): EDD does not include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
5. Information System Documentation (SA-5): EDD does not obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.
6. Software Usage Restrictions (SA-6): EDD does not comply with software usage restrictions.
7. User Installed Software (SA-7): EDD does not enforce explicit rules governing the installation of software by users.
8. Security Engineering Principles (SA-8): EDD does not design and implement the information system using security engineering principles.
9. External Information System Services (SA-9): EDD does not: (i) require that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.
10. Developer Security Testing (SA-11): EDD does not require that information system developers create a security test and evaluation plan, implement the plan, and document the results.

RISK: Strong system and services acquisition policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong system and services acquisition policy and procedures, EDD does not have a standardized approach to formally document and implement system and services acquisition policy and procedures.

Outsourced information system services protect information systems from unauthorized access by third-party providers.

Weak outsourced information services do not conform to the Agency's security policies; therefore, inadequate levels of information security may be implemented on the system, potentially allowing unauthorized access.

RECOMMENDATION: EDD Management should:

1. SA-1 System and Services Acquisition Policy and Procedures: Ensure the system services and acquisition policy addresses the purpose and scope of the control, and addresses roles, responsibilities, management commitment, coordination among agency entities, and compliance.
2. SA-2 Allocation of Resources: EDD management should determine security requirements for the information system in mission/business case planning. A discrete line item for information system security should be established in EDD's programming and budgeting documentation.
3. SA-3 Life Cycle Support: EDD management should manage the information system using a system development life cycle methodology that includes information security considerations.
4. SA-4 Acquisitions: Acquisition contracts for information systems should include, either explicitly or by reference, security requirements and/or security specifications that describe:
    a. -required security capabilities;
    b. -required design and development processes;
    c. -required test and evaluation procedures; and
    d. -required documentation.
5. SA-5 Information System Documentation: EDD management should obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.
6. SA-6 Software Usage Restrictions: EDD management should comply with software usage restrictions.
7. SA-7 User Installed Software: EDD management should enforce explicit rules governing the installation of software by users.
8. SA-8 Security Engineering Principles: EDD management should maintain the information system using security engineering principles consistent with NIST SP 800-27 and ensure developers are trained in how to develop secure software.
9. SA-9 External Information System Services: Ensure third-party providers are subject to the same information system security policy and procedures of the supported agency, and must conform to the same security control and documentation requirements as would apply to EDD's internal systems. Appropriate Agency officials approve outsourcing of information system services to third-party providers (e.g., service bureaus). The outsourced information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service level agreements. A service level agreement should be developed and approved that defines the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.
10. SA-11 Developer Security Testing: EDD management should require that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results for newly developed systems and modifications to existing systems that impact security controls.

AGENCY REPONSE: The EDD is in compliance with SA-1 through SA-4, and SA-8. The EDD's Mobile Computing Security Encryption Policy and Personal Computer Acquisition and Replacement Policy, along with policy issued by the Department of General Services establishes the framework that the EDD uses for System and Service Acquisition, Allocation of Resources, Life Cycle Support, Acquisitions, and Security Engineering Principles.

The EDD is in compliance with SA-6 and SA-7. Software usage is controlled and monitored utilizing the following automated tools: System Management Server - Microsoft, Active Directory (AD) - Microsoft, Trusted Enterprise Manager – Avatier, and Altiris - Symantec. A user is provided access to a specific information system at the desktop level via EDD's Employee Service Account Request (ESAR) process. This process requires that a desktop users' manager submit the ESAR to the Information Technology Branch (ITB) Service Desk. A Remedy ticket is then generated to ITB/Infrastructure Services Division whereby a user account is created with the requested authorization. The account is created in the AD and assigned to a 'global group' within the AD. Altiris manages the desktop image and software by using an enterprise software packaging and deployment approach. The EDD controls the desktop configuration/image via a Corporate (base) image and a Business Layer image for each user within EDD's enterprise. Desktop users do not have systems administrator or desktop administrator rights and privileges. Therefore, they cannot make changes or download software to their desktop workstations. If a device is identified via desktop monitoring/auditing of being non compliant with EDD's core image, that device will be re-imaged to meet departmental standards/controls.

The EDD is in compliance with SA-8 through SA-10 by our Change Management Policy, which sets and defines EDD's configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation. An Infrastructure Change Control Board meets weekly to review Change Requests. Some of the areas covered by the change requests are testing and security.

(See Attachments 11, 12, and 13)

IRS COMMENT: Agency response is partially accepted. Recommendations for SA-5 and SA-11 are not addressed in the agency response. Mitigating actions for SA-5 should be corrected within twelve months after receiving the Final SRR. Mitigating actions for SA-11 should be corrected within three months after receiving the Final SRR. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Management Controls – Certification & Accreditation

H.4 **FINDING:** Certification & Accreditation controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, seven Certification & Accreditation controls were found to not be compliant with IRS Publication 1075 standards. The non-compliant controls under the Certification & Accreditation control family include:

1. Certification, Accreditation, and Security Assessment Policies and Procedures (CA-1): EDD does not develop, disseminate, and periodically review/update: (i) formal, documented, security assessment policies that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and associated assessment controls.
2. Security Assessments (CA-2): EDD does not conduct an assessment of the security controls in the information system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
3. Information System Connections (CA-3): EDD does not authorize all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.
4. Security Certification (CA-4): EDD does not conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
5. Plan of Action and Milestones (CA-5): EDD does not develop and update a plan of action and milestones for the information system that documents the Agency's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls to reduce or eliminate known vulnerabilities in the system.
6. Security Accreditation (CA-6): EDD does not authorize (i.e., accredit) the information system for processing before operations and update the authorization at least every three years or when there is a significant change to the system. A senior organizational official does not sign and approve the security accreditation.
7. Continuous Monitoring (CA-7): EDD does not ensure continuous monitoring is ongoing at all times. Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. EDD management should establish the selection criteria for control monitoring and subsequently select a subset of the security controls employed within the information system for purposes of continuous monitoring.

RISK: Strong security assessment policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong security assessment policy and procedures, EDD does not have a standardized approach to formally document and implement these assessment policy and procedures.

Security assessments can include compliance testing and security risk assessments, which are performed on the system every three years or when there is a major change to the system. In addition, on an annual basis, a self-assessment is conducted on the system to evaluate its management, operational, and technical controls.

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation. It details the risks that are facing the system and to what extent the security controls are effective in mitigating those risks. Without a security certification, Agency officials lack the facts needed to render an accurate security accreditation decision.

A Plan of Action and Milestones (POA&M) is developed for systems to document the planned, implemented, and evaluated remedial actions to correct deficiencies identified during the assessment of the security controls in order to reduce or eliminate known vulnerabilities. Without a POA&M, corrective actions cannot be efficiently tracked and progress monitored for the system, thereby increasing the potential for weak system security.

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Without a system accreditation, Agency officials may not be fully aware of the security risks, technical constraints, operational constraints, and cost/schedule constraints facing a system, and therefore may not account for any adverse impacts to EDD if a breach of security occurs.

Continuous monitoring ensures that the system security controls are current and effective to address all current and newly identified threats and vulnerabilities. Without continuous monitoring, which includes configuration management activities and ongoing annual self-assessment of security controls, EDD may not have current evaluations of the system security controls implemented to protect against existing and future threats and vulnerabilities.

RECOMMENDATION: EDD management should:

1. CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures: Develop security assessment policy and procedures that are

consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The security assessment policies can be included as part of the general information security policy for the Agency. Security assessment procedures can be developed for the security program in general, and for a particular information system, when required.

2. CA-2 Security Assessments: Develop security assessments to support the requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be tested with a frequency depending on risk, but no less than annually.
3. CA-3 Information System Connections: EDD management should authorize all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.
4. CA-4 Security Certification: EDD management should conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Ensure the process is consistent with OMB policy and NIST Special Publications 800-37 and 800-53A.
5. CA-5 Plan of Action and Milestones: EDD management should ensure a POA&M is developed/updated based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The POA&M is a key document in the security package developed, and the POA&M is reviewed at least quarterly to address the elimination or acceptance of all risks identified.
6. CA-6 Security Accreditation: EDD management should authorize/accredit the information system for processing before operations and update the authorization in accordance with organization-defined frequency, at least every three years. Ensure a senior organizational official signs and approves the security accreditation. Ensure security accreditation process employed by the organization is consistent with NIST Special Publications 800-37 and that EDD updates the authorization when there is a significant change to the information system.
7. CA-7 Continuous Monitoring: EDD management should ensure continuous monitoring is ongoing at all times. Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. EDD establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring.

AGENCY REPONSE: The EDD is aware of the National Institute of Standards and Technology (NIST) Certification and Accreditation safeguard and controls for Information Technology Systems. The EDD's published audit and information security policy for ERM Framework includes the following standards: the EDD

Information Technology Governance Council adopted ERM best practices set forth by the Committee of Sponsoring Organizations (COSO) and the NIST for EDD's risk assessments and internal audit preparedness processes. The COSO standards are being used for programmatic portion of the risk assessments and the NIST standards are being used for IT portion of the risk assessments. The policy includes the Federal Information Security Management Act and the Federal Office of Management and Budget Circular A130-Appendix III.

(See Attachment 2)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Personnel Security

H.5 **FINDING**: Personnel Security controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: During an interview with a Human Resources representative it became clear that the department is following State of California agreements with its unions covering the matters of personnel handling. These procedures do not allow for sufficient investigation and suitability requirements for individuals with access to FTI data. The department did produce evidence of a suitable policy for termination and transfer of individuals with FTI access.

1. Personnel Security Policy and Procedures (PS-1): EDD does not develop, disseminate, nor periodically review/update: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
2. Position Categorization (PS-2): EDD does not assign a risk designation to all positions nor establish screening criteria for individuals filling those positions.
3. Personnel Screening (PS-3): EDD does not fully screen individuals requiring access to organizational information and information systems before authorizing access.
4. Personnel Sanctions (PS-8): EDD does not employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

RISK: Absent or weak personnel security policy and procedures could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system.

Absent or weak position categorization and personnel screening prevents EDD from determining that the appropriate personnel are assigned to the appropriate roles. Weak position categorization and personnel screening may potentially allow unauthorized access to the information system and the information.

Personnel screening helps the Agency determine the appropriate personnel are assigned to the appropriate roles. Weak personnel screening may potentially allow unauthorized access to the information and the information system.

An organization without a formal process for applying sanctions for individuals failing to comply with established information security policies and procedures promotes a general attitude that information security practices are of little importance to the individuals well being. Once that attitude is set in an individual or organization the discipline needed to produce a secure environment is gone and individuals will have little reason to comply with security requirements that cause extra work and extra efforts.

RECOMMENDATION: EDD Management should:

1. PS-1: Develop personnel security policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for EDD. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required.
2. PS-2: Ensure that position risk designations are consistent with applicable policy and guidance.
3. PS-3: Ensure that personnel screening is consistent with applicable policy, regulations, and guidance and the criteria established for the risk designation of the assigned position.
4. PS-8: The policy and rules of behavior documents should contain a formal sanctions process for personnel failing to comply with EDD information security policies and procedures.

AGENCY REPONSE: The EDD is in compliance with PS-1 through PS-3 and PS-8. The EDD provides annual training for all staff to ensure compliance.

(See Attachment 14)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Contingency Planning

H.6 **FINDING**: According to the on-site evaluation performed contingency planning controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: The agency did not produce evidence of contingency planning.

1. Contingency Planning Policy And Procedures (CP-1):
    a. Contingency planning policy and procedures do not (i) exist; (ii) are not documented; (iii) and not disseminated to appropriate elements within EDD.

   b. Contingency planning policy and procedures are not (i) periodically reviewed by responsible parties within EDD; and (ii) are not updated, when EDD review indicates updates are required.
   c. Contingency planning policy does not address the following areas: Alternate Storage Sites, Telecommunication Services, and Information System Backup.
2. Contingency Plan (CP-2):
   a. The ITCP does not address contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34.
   b. The contingency plan is not reviewed and approved by designated organizational officials, and disseminated to key personnel with contingency planning responsibility.
3. Contingency Plan Testing(CP-4):
   a. EDD does not define a set of contingency plan tests and/or exercises, and test/exercise the contingency plan annually.
   b. Testing records, such as after action reports, are not created to document the results of contingency plan testing/exercise. The ITCP is not updated based on the results of the test/exercise.
4. Contingency Plan Update (CP-5): EDD does not review the contingency plan for the information system.
5. Alternate Storage Site(CP-6): EDD did not identify an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.
6. Alternate Processing Site(CP-7): EDD did not identify an alternate processing site and the necessary agreements to permit the resumption of information systems operations for critical mission functions within EDD.

RISK: Strong contingency planning policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong contingency planning policy and procedures, EDD does not have a standardized approach to formally document and implement contingency planning policy and procedures.

RECOMMENDATION: EDD Management should:

1. CP-1: Contingency Planning Policy And Procedures
   a. Contingency planning policy and procedures should (i) exist; (ii) be documented; (iii) and be disseminated to appropriate elements within EDD.
   b. Contingency planning policy and procedures should (i) be periodically reviewed by responsible parties within EDD; and (ii) be updated, when EDD review indicates updates are required.

c. Contingency planning policy should address the following areas: Alternate Storage Sites, Telecommunication Services, and Information System Backup.

2. CP-2: Contingency Plan:
   d. The ITCP should address contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the information system consistent with NIST Special Publication 800-34.
   e. The contingency plan should be reviewed and approved by designated organizational officials, and disseminated to key personnel with contingency planning responsibility.
3. CP-4: Contingency Plan Testing:
   f. EDD management should define a set of contingency plan tests and/or exercises, and test/exercise the contingency plan annually.
   g. Testing records, such as after action reports, should be created to document the results of contingency plan testing/exercise. The ITCP should be updated based on the results of the test/exercise.
4. CP-5 Contingency Plan Update: EDD management should review the contingency plan for the information system.
5. CP-6 Alternate Storage Site: EDD management should identify an alternate storage site and initiate necessary agreements to permit the storage of information system backup information.
6. CP-7 Alternate Processing Site: EDD management should identify an alternate processing site and the necessary agreements to permit the resumption of information systems operations for critical mission functions within EDD.

AGENCY REPONSE: The EDD is in compliance with findings CP-1 through CP-7, as indicated below:

CP-1: Contingency Planning Policy and Procedures:

a. Continuity Plan For Business (CPB) Policy and Procedures do exist, are documented, and are disseminated to all appropriate branches within the EDD. The ISO is responsible for this implementation.
b. Contingency planning policy and procedures are periodically reviewed by the responsible parties within the EDD and are updated every May, in accordance with procedures as outlined by the ISO. The ISO is responsible for this implementation.
c. Contingency planning policy does address Alternate Storage Sites, Telecommunication Services, and Information System Backup. This information is located in Section 5 of the Enterprise CPB. The ISO is responsible for this implementation.

CP-2: Contingency Plan:

d. The ITB CPB outlines contingency roles, responsibilities, assigns individual with contact information and all activities for restoring the information systems consistent with the NIST Special Publication 800-34. This information is located in Section 5 of the Enterprise CPB for

the EDD. The ITB Continuity Management Office (CMO) has responsibility for this implementation.

e. The ITB CPB is updated yearly in May and reviewed for approval by the ISO, the ITB Deputy Director and all ITB Division Chiefs. The finalized ITB CPB is then disseminated to all key personnel including the ITB Deputy Director's Office, all ITB Division Chiefs, all Disaster Recovery Team leaders, and key team members. The ITB CMO has responsibility for this implementation.

CP-4: Contingency Plan Testing:

f. The EDD performs a yearly test of the hot site and ITB CPB in conjunction with the DTS. All major portions of the ITB CPB are tested for accuracy and effectiveness. Also smaller tests are scheduled annually outside the hot site test to highlight different portions of the ITB CPB for effectiveness review. The ITB CMO has responsibility for this implementation.

g. Testing records and Post Warm site Exercise Report was disseminated to all appropriate people for review and comment after the hot site test. Lessons learned from the report will be incorporated into the ITB CPB. The ITB CMO has responsibility for this implementation.

CP-5: Contingency Plan Update:

The ITB CPB is sent to the ITB Deputy Director and all ITB Division Chiefs for review, additions and comments before the final edition is disseminated to Recovery Team personnel. The ITB CMO has responsibility for this implementation.

CP-6: Alternate Storage Site:

The EDD currently has a contract with Iron Mountain through the DTS to provide secure off-site storage of our information system backups.

(See Attachment 19)

CP-7: Alternate Processing Site:

The EDD currently has a contract with International Business Machines through the DTS to provide an off-site processing site in Boulder, Colorado. In addition, the EDD central office has a contingency plan with the Tax Branch to provide an Alternate Work Site in the event that EDD's main offices in downtown Sacramento are unavailable for use due to disaster.

(See Attachment 20)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Configuration Management

H.7 FINDING: According to the on-site evaluation performed configuration management controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, five of the eight Configuration Management controls were found to not be compliant with IRS Publication 1075 standards. The five non-compliant controls under the Configuration Management control family include:

1. Configuration Management Policy and Procedures (CM-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
2. Monitoring Configuration Changes (CM-4): EDD does not monitor changes to the information system by conducting security impact analyses to determine the effects of the changes.
3. Configuration Settings (CM-6): EDD does not configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements. For example, the Mainframe with Top Secret had a number of configuration findings that are not consistent with IRS Publication 1075's recommendations.
4. Least Functionality (CM-7): EDD does not configure the information system to provide only essential capabilities and does not specifically prohibit and/or restrict the use of the functions, ports, protocols, and/or services EDD has determined are unacceptable risks.
5. Information System Component Inventory (CM-8): EDD has not developed, documented, or maintained a current inventory of the components of the information system with relevant ownership information.

RISK: Strong configuration management policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong configuration management policy and procedures, EDD does not have a standardized approach to formally document and implement configuration management policy and procedures.

Failure to analyze proposed or actual changes to the information system and determine the security impact of such changes before they are implemented may affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously.

Security configuration settings that ensure the system is configured to the most restrictive mode possible prevent unauthorized users from making unapproved changes to the system, thereby protecting system integrity. Lack of mandatory security configuration settings may result in exploitation without detection or user accountability.

Lack of access restriction may result in exploitation without detection or user accountability.

Lack of configuration settings may result in exploitation without detection or user accountability.

Least functionality settings closes all non-essential functionalities and services (e.g., prohibited or unused ports, protocols, services, voice over internet protocol, instant messaging, file transfer protocol, hyper text transfer protocol, file sharing, etc.). Failure to set systems to least functionality may increase system vulnerabilities and expose the system to malicious attacks.

RECOMMENDATION: EDD Management should:

1. CM-1 Configuration Management Policy and Procedures: Develop configuration management policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for EDD. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required.
2. CM-4 Monitoring Configuration Changes: EDD management should monitor changes to the information system by conducting security impact analyses to determine the effects of the changes.
3. CM-6: Configuration Settings: EDD management should ensure EDD records or documents show that the system is configured as follows: (i) mandatory configuration settings for information technology products employed within the information system are established; (ii) security settings of information technology products are configured to the most restrictive mode consistent with operational requirements; (iii) configuration settings are documented; and (iv) configuration settings in all components of the information system are enforced.
4. CM-7 Least Functionality: EDD management should ensure the system provides only the essential capabilities and prohibits any functionality that is not essential. Specifically the following protocols/services shall be disabled: (i) Network File System, (ii) Network Information System, (iii) Remote Procedure Call (RPC), (iv) Trivial File Transfer Protocol (TFTP), (v) User Datagram Protocol (UDP), (vi) boot services, (vii) r-commands, (viii) Routing Information Protocol (RIP), (ix) daemon (routed), and (x) Internet Control Message Protocol (ICMP) redirects. Ensure all prohibited ports, protocols, and services are disabled.

5. CM-8 Information System Component Inventory: EDD management should develop, document, and maintain a current inventory of the components of the information system with relevant ownership information.

AGENCY REPONSE: The EDD is in compliance with CM-1 through CM-8. The EDD's Production Change Management Process covers all aspects of Configuration Management, Configuration Changes, and Configuration Settings. Least Functionality (CM-7) is addressed in EDD's Production Change Management Process and in EDD's Information Security Policy. Information System Component Inventory (CM-8) is developed, documented, and maintained by the EDD's Cost and Resources Management Section and the Enterprise Architecture Office.

(See Attachments 16 and 8)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Maintenance

H.8 **FINDING**: According to the on-site evaluation performed maintenance controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, three of the eight Maintenance controls were found not to be compliant with IRS Publication 1075 standards. The three non-compliant controls under the Configuration Management control family include:

1. System Maintenance Policy and Procedures (MA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
2. Maintenance Tools (MA-3): EDD does not approve, control, and monitor the use of information system maintenance tools nor maintain the tools on an ongoing basis.

3. Remote Maintenance (MA-4): EDD does not approve, control, and monitor remotely executed maintenance and diagnostic activities. Telnet is used for remote maintenance of the system. Additionally, the vendor can remotely access the system through the telephone directly connected to the mainframe.

RISK: Strong system maintenance policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong system maintenance policy and procedures, the Agency does not have a

standardized approach to formally document and implement system maintenance policy and procedures.

The use of approved maintenance tools on an ongoing basis helps to ensure information system equipment continues to operate correctly. Without proper maintenance tools, the risk of unauthorized or inappropriate changes to the equipment or system increases.

Remote maintenance controls help ensure any remotely executed maintenance and diagnostic activities are performed in accordance with all Agency maintenance policy and procedures. Weak remote maintenance controls may potentially allow unauthorized access to the information system or the information the system processes, stores, or transmits.

RECOMMENDATION: EDD management should:

1. MA-1 System Maintenance Policy and Procedures: Develop information system maintenance policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the Agency. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required.
2. MA-3 Maintenance Tools: Ensure all maintenance tools policy and procedures adequately address the use of maintenance tools. Ensure that maintenance tools used to perform system maintenance are approved and use of the tools is monitored.
3. MA-4 Remote Maintenance: Ensure EDD approves, controls, and monitors remotely executed maintenance and diagnostic activities. Maintenance logs are maintained for all remote maintenance, diagnostic, and service activities. Appropriate Agency officials periodically review maintenance logs. When remote maintenance is completed, the information system should terminate all sessions and remote connections. Telnet is not used for remote maintenance.

AGENCY REPONSE: The EDD is in compliance with MA-1 through MA-4. System Maintenance, Maintenance Tools, and Remote Maintenance are covered in EDD's Information Security Policy and the Employee Access Control Policy.

(See Attachments 8 and 17)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – System and Information Integrity

H.9 **FINDING:** System & Information Integrity controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, six System and Information Integrity controls were found not to be compliant with IRS Publication 1075 standards. The six non-compliant controls under the System and Information Integrity control family include:

1. System And Information Integrity Policy And Procedures (SI-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
2. Malicious Code Protection (SI-3): EDD does not implement malicious code protection.
3. Information System Monitoring Tools and Techniques (SI-4): EDD does not employ tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.
4. Security Alerts and Advisories (SI-5): EDD does not receive information system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.
5. Information Input Restrictions (SI-9): EDD does not restrict the capability to input information into the system to authorized individuals.
6. Information Output Handling and Retention (SI-12): EDD does not handle and retain output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

RISK: Strong system and information integrity policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong system and information integrity policy and procedures, EDD does not have a standardized approach to formally document and implement system and information integrity policy and procedures.

Information system monitoring tools and techniques help to detect any system intrusions. Without employing appropriate monitoring tools and techniques, the information system may be slow to detect intrusions and become more vulnerable to attacks.

Failure to receive information system security alerts/advisories on a regular basis may hamper the Agency's ability to improve knowledge of security best practices and react accordingly to mitigate exploitable vulnerabilities.

RECOMMENDATION: EDD Management should:

1. SI-1 System and Information Integrity Policy and Procedures: EDD management should develop system and information integrity policy and procedures that are consistent with the IRS Publication 1075 and applicable

federal laws, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for EDD. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required.

2. SI-2 Malicious Code Protection: EDD management should ensure a process is in place to identify recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the system. Ensure newly released security patches, service packs and hot fixes are installed on the information system in a reasonable timeframe in accordance with agency policy and procedures, and after being tested in a test environment.
3. SI-3 Information System Monitoring Tools and Techniques: EDD management should ensure EDD employs virus protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network that store, process or transmit FTI. Ensure virus protection mechanisms are configured to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) transported: by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., diskettes or compact disks), or other common means. Ensure the virus protection mechanisms (including the latest virus definitions) are updated whenever new releases are available, and the virus protection mechanism automatically updates its malicious code definitions. Ensure consideration is given to using virus protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).
4. SI-4 Security Alerts and Advisories: EDD management should ensure the information system has intrusion detection capability. The intrusion detection tools are configured and updated to detect vulnerabilities, changes to the network, both known and unknown attack signature, and traffic anomalies.
5. SI-9 Information Input Restrictions: EDD management should ensure restrictions are employed for personnel authorized to input information to the information system to include limitations based on specific operational/project responsibilities. User accounts should be restricted from inputting information beyond the typical access controls unless specifically authorized based on operational/project responsibilities.
6. SI-12 Information Output Handling and Retention: EDD management should ensure EDD retains output from the information system in accordance with Agency policy and operational requirements/procedures. EDD management should handle output from the information system according to the system marked instructions and Agency policy and operational procedure and operational requirements/procedures.

AGENCY REPONSE: The DTS implements "Malicious Code Protection," including protection from viruses, worms, Trojan horses, and spyware, at various points in the network infrastructure and on applicable hosts. The DTS deploys malicious code protection that blocks incoming malicious e-mail at the email gateways. The DTS deploys host-based malicious code protection on Windows

servers and desktops. The DTS does not deploy malicious code protection on those platforms where it is not considered a significant threat (e.g. UNIX including AIX, and Z/OS). The DTS' Intrusion Prevention System (IPS) also blocks some malicious codes. The specific IPS protection varies depending on the network location.

The DTS has a proactive detection and remediation program for security vulnerabilities. When advisories are received they are analyzed and systems updated if appropriate. This is documented in DTS' policy "3300 Vulnerability Management Policy."

(See Attachment 7)

IRS COMMENT: Agency response is partially accepted. The agency's response does not address SI-9 or SI-12. SI-9 mitigating recommendations should be corrected within six months after receiving the Final SRR. SI-12 mitigating recommendations should be corrected within three months after receiving the Final SRR. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Operational Controls – Incident Response and Incident Reporting

H.10 FINDING: Incident Response and Incident Reporting controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, seven of the Incident Response and Incident Reporting controls were found to not be compliant with IRS Publication 1075 standards. The seven non-compliant controls under the Incident Response and Incident Reporting control family include:

1. Incident Response Policy and Procedures (IR-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
2. Incident Response Training (IR-2): EDD does not train personnel in their incident response roles and responsibilities with respect to the information system and does not provide refresher training annually.
3. Incident Response Testing and Exercises (IR-3): EDD does not test and/or exercise the incident response capability for the information system annually using Agency-defined tests and/or exercises to determine the incident response effectiveness and document the results.
4. Incident Handling (IR-4): EDD does not implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

5. Incident Monitoring (IR-5): EDD does not track and document information system security incidents on an ongoing basis.
6. Incident Reporting (IR-6): EDD does not promptly report incident information to appropriate authorities.
7. Incident Response Assistance (IR-7): EDD does not provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

RISK: Strong incident response policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong incident response integrity policy and procedures, EDD does not have a standardized approach to formally document and implement incident response policy and procedures.

Incident response training provides necessary instructions to personnel when security incidents need to be reported. Failure to provide incident response training may prevent effective and efficient reporting efforts of security breaches. Failure to test and/or exercise the incident response capability may hamper the Agency's ability to be prepared for actual emergency situations related to the IT plan.

Lack of a well developed incident handling policy cripples an Agency's ability to best respond to and manage adverse situations involving the information system. Incident handling policies and procedures will promote more efficient utilization of capabilities in responding to cyber attacks.

Incident monitoring ensures inappropriate or unusual activity is reported to management, local security personnel, and network security and the incident is appropriately documented and tracked. Failure to provide incident monitoring controls may prevent effective and efficient reporting efforts of security breaches.

Lack of a well developed incident reporting policy cripples an Agency's ability to best respond to and manage adverse situations involving the information system. Incident reporting policies and procedures will promote more efficient utilization of capabilities in responding to cyber attacks.

Incident response assistance provides a way for users to report incidents and for the appropriate response and assistance to be provided to aid in recovery.

RECOMMENDATION: EDD management should:

1. IR-1 Incident Response Policy and Procedures: Develop incident response policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the Agency. Incident response

procedures can be developed for the security program in general, and for a particular information system, when required.

2. IR-2 Incident Response Training: Ensure personnel are trained on their incident response roles and responsibilities. EDD management should ensure inappropriate or unusual activity is reported to management, local security personnel, and network security.
3. IR-3 Incident Response Testing and Exercises: EDD management should test and exercise the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency. Ensure tests/exercise results are documented. NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.
4. IR-4 Incident Handling: Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly. Ensure the incident handling capability is consistent with NIST Special Publication 800-61. NIST Special Publication 800-83 provides guidance on Malware incident handling and prevention.
5. IR-5 Incident Monitoring: Ensure that personnel are provided mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. Ensure all incidents are appropriately documented and progress tracked.
6. IR-6 Incident Reporting: Ensure weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. Ensure the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. NIST Special Publication 800-61 provides guidance on incident handling and reporting.
7. IR-7 Incident Response Assistance: Provide an incident response support resource that offers advice and assistance to information system users. Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

AGENCY REPONSE: The EDD is in compliance with IRS' recommendation regarding the policies for handling, monitoring, and reporting incidents and the response to the incident.

(See Attachment 18)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Operational Controls – Awareness and Training

H.11 **FINDING**: Security training and awareness controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, one of four Awareness and Training controls were found to be compliant with IRS Publication 1075 standards. The three non-compliant controls under the Incident Response and Incident Reporting control family include:

1. Security Awareness and Training Policy And Procedures (AT-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
2. Security Awareness (AT-2): EDD does not ensure all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and annually thereafter.
3. Security Training (AT-3): EDD does not identify personnel with significant information system security roles and responsibilities, document those roles and responsibilities, and provide appropriate information system security training before authorizing access to the system and annually thereafter.

RISK: Strong security awareness and training policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong security awareness and training policy and procedures, EDD does not have a standardized approach to formally document and implement security awareness and training policy and procedures.

Security awareness provides personnel and contractor employees involved with the management, operation, programming, maintenance, or use of Agency information systems with the necessary security basics to promote a responsible and secure operating environment. Weak security awareness controls may potentially allow unauthorized access (intentional or unintentional) to the information system or the information the system processes, stores, or transmits.

Security training controls provides personnel and contractor employees involved with the management, operation, programming, maintenance, or use of Agency information systems with the necessary security basics to promote a responsible and secure operating environment. Without formally documented and established roles and responsibilities, appointed personnel may not know or fully understand their expectations and/or functional limitations. Weak security training controls may potentially allow unauthorized access (intentional or unintentional) to the information system or the information the system processes, stores, or transmits.

RECOMMENDATION: EDD management should:

1. AT-1 Security Awareness and Training Policy and Procedures: Develop security awareness and training policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the Agency. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required.
2. AT-2 Security Awareness: Ensure the development of appropriate security awareness content and training material based on the specific requirements of EDD and the information system to which personnel have authorized access. Conduct the security awareness training before the users can access the information systems and continue annually thereafter. EDD management should determine the appropriate content of security awareness training based on the specific requirements of EDD and the information systems to which personnel have authorized access.
3. AT-3 Security Training: Identify appropriate personnel with significant information system security roles and responsibilities. Document those roles and responsibilities, and conduct appropriate information system security training before authorizing access to the system, and periodically conduct the security training thereafter. EDD management should determine the appropriate content of security training based on the specific requirements of EDD and the information systems to which personnel have authorized access. In addition, EDD management should ensure system managers, system administrators, and other personnel who have access to system-level software have adequate technical training to perform their assigned duties.

AGENCY REPONSE: The EDD is in compliance with IRS' recommendation.

(Refer to D.1 of the IRS Safeguard Review Report dated June 2008.)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technical Controls – Identification and Authentication

H.12 FINDING: Identification and authentication controls are implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, five of the Identification and authentication controls were found not to be compliant with IRS Publication 1075 standards.

1. Identification And Authentication Policy And Procedures (IA-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented

procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

2. Device Identification and Authentication (IA-3) EDD's information system does not identify and authenticate specific devices before establishing a connection.
3. Identifier Management (IA-4): EDD does not manage user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate Agency official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after 90 days of inactivity; and (vi) archiving user identifiers. User account management policy and procedures do not exist but informal processes seem to be in place.
4. Authenticator Management (IA-5): EDD does not manage information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authentication distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.
5. Cryptographic Module Authentication (IA-7): The EDD information system does not employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

RISK: Strong identification and authentication policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong identification and authentication policy and procedures, the Agency does not have a standardized approach to formally document and implement identification and authentication policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

Identifier management allows an Agency to protect itself from possible exploitation of the identifier creation process. Failure to implement this security control could lead to unauthorized access to the information system resulting in irreversible and detrimental harm to information system data, users and assets.

RECOMMENDATION: EDD management should:

1. IA-1 Identification And Authentication Policy and Procedures: Develop identification and authentication policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the Agency. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required.

2. IA-3 Device Identification and Authentication: EDD's information system should identify and authenticate specific devices before establishing a connection.
3. IA-4 Identifier Management: Establish an identifier management procedure to:
   1) Uniquely identify each user;
   2) Verify the identify of each user;
   3) Designate appropriate Agency officials that shall issue authorizations for the establishment of information system user accounts;
   4) Ensure that the user identifier and information system access credentials are issued to the intended party in such a manner so as to prevent compromising the confidentiality of the credentials;
   5) To disable user access to the information system after a 90 day period of inactivity;
   6) Assure that user identifiers are archived, and that those archives are kept secure.
4. IA-5 Authenticator Management: EDD management should manage information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authentication distribution, for lost, compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.
5. IA-7 Cryptographic Module Authentication: The EDD information system should employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

AGENCY REPONSE: The EDD has a documented Employee Access Control Policy. The policy addresses the purpose, scope, responsibilities, standards, and requirements. This policy is provided to program managers, system and network administrators, system application developers, and EDD staff. The policy discusses a uniform, consistent approach to design, implement, and maintain data integrity and information security in systems and applications.

The EDD is in compliance with IRS' recommendation. The EDD prohibits the use of external connections such as modems, wireless networks, dialup connections, wireless devices, etc. without written approval from the ITB Deputy Director and Information Security Officer. The approval is based on a risk analysis, risk mitigation plan, and individual authentication plan that ensure appropriate information security. (Reference: EDD Employee Access Control Policy – pg.6)

Numbers 1-4 – The EDD is in compliance with IRS' recommendation. All individuals provide identification and authentication in the form of a unique Identification (UserID) and password before accessing EDD sensitive or confidential information. The EDD prohibits the use of group and shared passwords. (Reference: EDD Employee Access Control Policy – pg.7)

Number 5 – The EDD is in compliance with IRS' recommendation. (Reference: Information Systems Standards and Procedures Manual – UserID standards [Screen 10])

- The UserID that has never been used will be deleted after 3 months;
- The UserID that has not had any activity for 90 days will be automatically inactivated.

(See Attachment 17)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technical Controls – Access Control

H.13 FINDING: According to the on-site evaluation performed access controls are not implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, seven of the Identification and authentication controls were found not to be compliant with IRS Publication 1075 standards.

1. Access Control Policy and Procedures (AC-1): EDD management has not developed, disseminated, or reviewed (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
2. Account Management (AC-2): EDD does not manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. EDD does not review information system accounts at lest annually.
3. Least Privilege (AC-6): The EDD information system does not enforce the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
4. Unsuccessful Login Attempts (AC-7): The EDD information system does not enforce a limit of 3 consecutive invalid access attempts by a user during a 15 minute time period. The information system does not automatically lock the account for a 15 minute time period, nor delay the next login prompt for 15 minutes when the maximum number of unsuccessful attempts is exceeded.
5. System Use Notification (AC-8): The EDD information system does not display an approved system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring. The system use notification message does not provide appropriate privacy and security notices based on IRS requirements.

6. Session Lock (AC-11): The EDD information system does not prevent further access to the system by initiating a session lock after 15 minutes of inactivity until the authorized user reestablishes access using appropriate identification and authentication procedures.
7. Session Termination (AC12): The EDD information system does not automatically terminate a remote session after 15 minutes of inactivity.

RISK: Strong access control policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong access control policy and procedures, the Agency does not have a standardized approach to formally document and implement access control policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

Managing information system accounts - to include the individual aspects of the management process - are essential to the security of the information system as it allows administrators to restrict access solely to authorized parties, identify who those parties are, and to exercise authority over the security controls governing the access restrictions of these parties. Failure to manage information system accounts or review them on a frequent basis can result in unauthorized access to information system resources and eliminate any ability to enforce accountability for information system misuse. Failure to employ automated mechanisms to support the management of information system accounts increases the possibility of human error. Failure to automatically terminate temporary and emergency accounts, or to automatically disable inactive accounts after a period of time can result in unauthorized access through exploitation of these accounts. Because these accounts are not periodically reviewed, the unauthorized access will continue indefinitely.

Enforcing the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks mitigates the risk that authorized personnel are conducting unauthorized activities on or with the information system. Failure to enforce the most restrictive set of rights/privileges for users on the information system can lead to exploitation and compromise of the security and functionality of the information system.

Enforcing a limit on the number of consecutive access attempts by a user within a time period which would result in temporary lockout when the limit is met assures that unauthorized users attempting to access authorized users' information system accounts are prevented from doing so. Failure to enforce a limit on the number of consecutive access attempts by a user can facilitate an unauthorized user's attempts to "brute force" their way into an authorized user's account by guessing an indefinite number of passwords until the valid one is uncovered.

Displaying an approved system use notification message which informs potential users that the information system is the property of the U.S. Government, that usage on it may be monitored, that unauthorized use of the system may result in criminal or civil penalties, and that use of the system indicates consent to monitoring, informs the end user of the responsibilities they have when accessing the system and when using it, and of the consequences of unauthorized access or use of the information system. Without this banner, Agencies may have no legal recourse to monitor an end user's actions or discipline an end user for violating the Agency's rule of behavior.

Documenting, monitoring and controlling all methods of remote access to the information system is necessary in that it applies the same level of security protection to forms of remote access as are implemented on forms of local access. Failure to document, monitor and control all methods of remote access leaves the information system vulnerable to attack from an outside unauthorized party. Failure to employ automated mechanisms to facilitate the monitoring and control of remote access methods leaves the information system vulnerable to human error. Failure to use encryption to protect the confidentiality of remote access sessions can result in data interception by an unauthorized third-party eavesdropping on a remote connection between the information system and an authorized user. Failure to control all remote accesses through a managed access control point creates difficulty in assuring that all remote accesses are subject to the same level of security.

Terminating a session after a period of inactivity is necessary in that it decreases the possibility that an unauthorized user will seize control of the session. Failure to terminate a session after a period of inactivity makes it likely that a passing user might take control of the session on the device that has been apparently abandoned and have access to FTI data.

RECOMMENDATION: EDD Management should:

1. AC-1: Develop access control policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for EDD. Access control procedures can be developed for the security program in general, and for a particular information system, when required.
2. Account Management (AC-2): Minimize manual review processes and decrease risk by implementing system-based controls that:
    a. automatically disables inactive and accounts after the account reaches the defined period of inactivity;
    b. automatically disables temporary accounts based on the defined period temporary accounts are permitted to exist.
3. Least Privilege (AC-6): EDD management should enforce the concept of least privilege by:
    a. Assign only the absolute minimum level of access necessary to users in order to conduct their tasks;

b. Develop a procedure so that authorization for any increase in functionality should come only through approved channels.

4. Unsuccessful Login Attempts (AC-7): The EDD information system should ensure that all information system accounts are configured to be disabled for a certain period of time, or until the authorized user contacts an official or Agency authorized to reinstate account access, in the event that a consecutive invalid access attempts is reached. If possible, enable a mechanism which would inform the user upon exceeding this limit, or upon further attempts to authenticate (or both) of how to reinstate account access.
5. System Use Notification (AC-8): The EDD information system should implement a system use notification message to be displayed before granting system access which informs users that the information system is the property of the U.S. Government, that use of the system may be monitored, that unauthorized use of the system may result in criminal or civil penalties, and that use of the system indicates consent to monitoring. Such language should be composed by general counsel, or the language provided in agency/department wide policy should state, that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and that use of the system indicates consent to monitoring. The message must be in accordance with stipulations in IRS Publication 1075.
6. Session Lock (AC-11): The EDD information system should implement a session lock that is activated after a defined period of computer inactivity and remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
7. Session Termination (AC12): The EDD information system should automatically terminate a remote session after 15 minutes of inactivity.

AGENCY REPONSE: When one's workstation is left unattended for an extended period, individuals must: (Reference: EDD Employee Access Control Policy – pg.
6)

a. Terminate active sessions when finished, unless they are secured by an appropriate locking mechanism; e.g., a password protected screen saver;
b. Secure personal computers (PC) or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use;
c. Use the "Lock Workstation" function anytime they leave their immediate areas (applies to Windows NT and 2000);
d. Individuals with workstations running Windows 95 must execute the "Shutdown-Log on as another individual" function anytime they leave their immediate work area; and
e. Follow instructions outlined in the Information Technology Circular (ITC) 01-08C "Re-issuance of the Desktop Security Screen Saver Feature Requirement."

The EDD has a documented Employee Access Control Policy that addresses consistent protection of data integrity and information security of all programs, systems, and business applications within the EDD. Before individuals are granted access rights, they must complete their information security training,

locally required training, and sign the appropriate nondisclosure agreements. Each automated information session must start with the person establishing their identity and authorizations (unique personal identifier and password).

(See Attachment 17)

IRS COMMENT: Agency response is partially accepted. The agency's response and the attachment do not adequately address the AC-2, AC-7, and AC-8 recommendations. AC-2, AC-7, and AC-8 recommended mitigations should be corrected within three months after receiving the Final SRR. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Technical Controls – Auditing

H.14 FINDING: Audit & Accountability controls are not being implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, six Audit & Accountability controls were found to not be compliant with IRS Publication 1075 standards. The non-compliant controls under the Audit & Accountability control family include:

1. Audit And Accountability Policy And Procedures (AU-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
2. Auditable Events (AU-2): The EDD information system does not generate audit records for the events as required in IRS Publication 1075.
3. Content Of Audit Records (AU-3): The EDD information system does not produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
4. Response To Audit Processing Failures (AU-5): The EDD information system does not alert appropriate organizational officials in the event of an audit processing failure and EDD has not defined the activities the system should take.
5. Audit Reduction And Report Generation (AU-7): The EDD information system does not provide an audit reduction and report generation capability.
6. Time Stamps (AU-8): The EDD information system does not provide time stamps for use in audit record generation.

RISK: Strong audit and accountability policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without strong audit

and accountability policy and procedures, EDD does not have a standardized approach to formally document and implement audit and accountability policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

RECOMMENDATION: EDD Management should:

1. AU-1 Audit And Accountability Policy And Procedures: Develop audit and accountability policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for DSS. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required.
2. AU-2 Auditable Events: Develop, document and continuously update a list of all auditable events. Configure the information system so that it can record these events per the IRS Publication 1075 policy. Include in this list of auditable events, procedures for compiling and distributed the audit records to the necessary parties for review.
3. AU-3 Content Of Audit Records: Develop and document a list of required information for auditing logging that provides sufficient information for the Agency to determine what occurred, the source, and the outcome of the events. Using this list, determine if this capability exists within the information system.
4. AU-5 Response To Audit Processing Failures: Provide sufficient storage capacity to capture records based on Agency guidance and best practices. In addition, configure automatic notifications are implemented and functional so that there is no failure in the notification of Agency officials in the event of an audit failure or storage capacity being reached.
5. AU-7 Audit Reduction and Report Generation: The EDD management should acquire an audit reduction and reporting tool.
6. AU-8 Time Stamps: Configure the audit logging functionality of the information system to include time stamps as part of the audit record (a good rule of thumb for the content of audit records is to ensure that "who", "what", "where", "when", and "how" are addressed). In addition, the Agency should configure all information systems to synchronize to a central NTP server so that one time is used for all IT assets with clocks.

AGENCY REPONSE: The EDD has established a concept to develop an Audit Logging program similar to the State of California's Franchise Tax Board. A Budget Change Proposal to authorize the necessary funds for this program is also under development. The EDD will provide the IRS with Quarterly updates regarding the status of this Corrective Action Plan.

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technical Controls – System & Communications Protection

H.15 **FINDING:** System & Communications Protection controls are not being implemented according to IRS Publication 1075 standards.

DISCUSSION: According to the on-site evaluation performed, five System & Communications controls were found not to be compliant with IRS Publication 1075 standards. The non-compliant controls under the System & Communications control family include:

1. System And Communications Protection Policy And Procedures (SC-1): EDD does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
2. Information Remnance (SC-4): EDD does not prevent unauthorized and unintended on formation transfer via shared system resources.
3. Information Integrity (SC-8): EDD's information system does not protect the integrity of transmitted information.
4. Transmission Confidentiality (SC-9): EDD's information system does not protect the confidentiality of transmitted information.
5. Network Disconnect Control (SC-10): EDD's system does not terminate a network connection at the end of a session or after 15 minutes of inactivity.

RISK: Strong system and communications protection policy and procedures ensure adequate security (commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or assets supporting the system). Without system and communications protection policy and procedures, EDD does not have a standardized approach to formally document and implement system and communications protection policy and procedures. This may lead to disparate operating processes that result in increased security exposures.

RECOMMENDATION: EDD Management should:

1. SC-1 System And Communications Protection Policy And Procedures: Develop system and communications protection policy and procedures that are consistent with the IRS Publication 1075 and applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the Agency. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required.
2. Information Remnance (SC-4): Configure and document procedures for the information system regarding the use of encryption for data transmitted over an unsecured network. EDD management should ensure that it is FIPS 140-2 compliant.

3. Information Integrity (SC-8): EDD's information system shall institute a procedure to securely verify that all transmissions have integrity checks, that is, the recipient is assured that what they receive is what was sent.
4. Transmission Confidentiality (SC-9): EDD's information system shall protect the confidentiality of transmitted information, by having all transmissions encrypted with an approved protocol or installing another acceptable system, such as total fiber optics within an enclosed and protected area.
5. Network Disconnect Control (SC-10): EDD's system settings should terminate a network connection at the end of a session or after 15 minutes of inactivity.

AGENCY REPONSE: The EDD is in compliance with SC-1, SC-4, SC-8, SC-9 and SC-10. The EDD Information Security Policy protects EDD information, communications, networks, systems, applications, equipment, facilities, and other information assets and sets the information security standards as summarized below:

1. Information Security Policy
2. Organization Security
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Automated Systems Development and Maintenance
9. Business Continuity Planning Management
10. Compliance

The EDD Employee Access Control Policy further protects the network by providing system disconnect controls.

Policy Statement:
The EDD Employee Access Control Policy ensures consistent protection of data integrity and information security of all programs, systems, and business applications within the EDD. Before individuals are granted access rights, they must complete their information security training, locally required training, and sign the appropriate non-disclosure agreements. Each automated information session must start with the person establishing their identity and authorizations (unique personal identifier and password).

(See Attachments 8 and 17)

IRS COMMENT: Agency response is accepted. No further direction is needed.

Technology Specific Findings

A representative sample of platforms (see completed SCSEMs for the list of names) was tested to drive the findings listed in this section. Although the findings were identified on the specific platforms tested, corrective actions recommended for each technology in this report should be tested and implemented on ALL platforms (with the same technology) that store, transmit, or process FTI.

Identification & Authentication – AIX

H.16 **FINDING:** According to the on-site evaluation performed password control at the system level is inadequate.

DISCUSSION: Discussion with system administrators revealed that the system level password controls are inadequate.

1. System level passwords are not set to have aging.
2. System level passwords are not required to meet standards of password length.
3. System level passwords are able to reset to any previous password.
4. System level individuals do not receive a password expiring notice.
5. System level passwords are not checked against standard vulnerable passwords.

RISK: The risk in having weak passwords, particularly at the system level, is that any individual with access to the system at the administrative level should have little difficulty in gaining control of the system with its FTI data in a minimum of time. Although it is the case that physical access to administrative terminals is restricted by location it is possible for an individual to gain access via the network. Even if the discussion concerns only individuals with system administrative rights it is relatively easy for such a administrator to use the identity of another system administrator to compromise the system and its FTI.

RECOMMENDATION: EDD Unix administrators should ensure that:

1. Passwords shall be changed every 90 days, at a minimum, for standard user accounts to reduce the risk of compromise through guessing, password cracking or other attack & penetration methods. Passwords shall be changed every 60 days, at a minimum, for privileged user accounts to reduce the risk of compromise through guessing, password cracking or other attack and penetration methods. Set maxage=90
2. Passwords shall be a minimum length of 8 characters in a combination of alpha and numeric or special characters. Set minlen=8, minalpha=8
3. Users shall be prohibited from using their last six passwords to deter reuse of the same password. Set histexpir=6
4. The information system shall routinely prompt users to change their passwords within 5-14 days before such password expires. Set pwdwarntime=14
5. Use of dictionary words, popular phrases, or obvious combinations of letters and numbers in passwords shall be prohibited when possible.

Obvious combinations of letters and numbers include first names, last names, initials, pet names, user accounts spelled backwards, repeating characters, consecutive numbers, consecutive letters, and other predictable combinations and permutations. Use a password checker on the password file.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.17 **FINDING**: According to the on-site evaluation performed the information system protects audit information and audit tools from unauthorized access, modification, and deletion.

DISCUSSION: Access to the audit information is available to root. For operational requirements that access to su root lies only with system administrators and data base administrators.

RISK: The risk of having access to audit data not held extremely close is that audit data can then be manipulated by unauthorized individuals. A compromise of the audit records:

1. makes reliance on audit records impossible
2. unreliable audit records make the identification of the cause of disruptive or unauthorized acts on the system extremely difficult
3. unreliable audit records make the tracking of FTI exposure unreliable
4. an unreliable audit record makes findings inadmissible as evidence in a prosecution or adverse personnel action.

RECOMMENDATION: None. All requirements are met.

Access Control – AIX

H.18 **FINDING**: According to the on-site evaluation performed the organization does not review information system accounts to ensure that existing accounts are being controlled properly as required by IRS Publication 1075.

DISCUSSION: The UNIX administrators stated that they do not review accounts on a routine basis. It was their feeling that they knew everyone with access to their system and that such a periodic review was unnecessary.

RISK: The risk associated with a failure to review system accounts lies in the real possibility of having an individual account which should no longer have access remain active. If this account has no authorized user it could be exploited by another individual to access system resources. Activity on such an account would likely go unnoticed since the account had been authorized. Leaving accounts on any system when they are no longer authorized exposes the system and the FTI data it contains.

RECOMMENDATION: EDD management should establish a written policy which requires periodic and systematic review of all accounts on any system which manipulates, stores, or has any access to FTI material system. EDD management must have required audits performed and documented. Audit logs should be sent to a logger file (e.g. logger.edd.ca.gov), reviewed and rotated on a regular basis. All logs passed to the logger should be parsed on a routine basis via cron with a program such as logcheck.sh. The logs should include:

1. authlog
2. cronlog
3. daemonlog
4. lprlog
5. kernlog
6. newslog
7. sudo.log
8. tcpwrap.log
9. syslog.log
10. mail.log
11. ssh.log

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.19 **FINDING**: According to the on-site evaluation performed the agency does not adhere to the principle of least privilege when creating user accounts. EDD has not controlled the issuance of authorizations using the least privilege tenants.

DISCUSSION: The principle of least privilege is used when creating users and groups on the UNIX system. Industry standard practice is to create user ID and group ID permissions using UNIX Access Control Lists (ACLs) in AIX. EDD fails to exercise least privilege in that all accounts at the system level are assigned access to all administrative rights. Assignment of users to the application program is administered by the application program.

RISK: The risk in not checking the authorization levels for users and assigning users all equally powerful rights is that individuals will have control over the system that exceeds their level of responsibility. This increases the probability of deliberate or inadvertent introduction of harmful procedures that can damage the system and expose FTI material. Control of all user accounts should be controlled by the system administrator.

RECOMMENDATION: EDD management should create a written policy stating the levels of system access to be granted to individual roles. The system administrators should create procedures to implement that policy. The system administrators should control all user access to the system and to any applications residing on the system. System administrators should coordinate with the application owners and the data owners to establish procedures for granting access to the application and FTI data.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the

Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.20 **FINDING:** According to the on-site evaluation performed the system does not display an appropriate warning banner before authentication.

DISCUSSION: The system is not configured to display a logon banner containing any information about the sensitivity, confidentiality, or the consequences for misuse of the system.

RISK: A warning banner serves two purposes. First, it is a tool to warn a would-be attacker that they are attempting to access a government resource and their actions will be monitored. Second, it is a tool to help aid prosecution of attackers that have compromised a system. If the banner doesn't cover these two areas an attacker could potentially avoid prosecution by claiming they weren't aware they were accessing a government computer system.

RECOMMENDATION: The EDD Unix administrator should set a warning banner for the following system directories: /etc/motd, /etc/issue, and /etc/security/login.cfg. The banner should identify that the system is for authorized users only, user activity is monitored, and that improper use of the system will result in Federal/State criminal and/or civil penalties. The warning banner language should speak to both authorized and unauthorized users, which would cover malicious insider users as well as attackers from outside. The warning banner shown before a successful connection to all network devices should be similar to the following:

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.

If the device can only support a short banner, the contents of the banner should be:

WARNING! US GOVERNMENT SYSTEM. Unauthorized access prohibited by Public Law 99-474 "The Computer Fraud and Abuse Act of 1986". Use of this

system constitutes CONSENT TO MONITORING AT ALL TIMES and is not subject to ANY expectation of privacy.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Auditing – AIX

H.21 **FINDING**: According to the on-site evaluation performed the UNIX audit logs are not capturing events as required by IRS Publication 1075 standards.

DISCUSSION: Discussion with the system chief administrator revealed that at the system level only login and logout records are kept in the system audit trail. The system administrator explained that the system is accessed by only a few system administrators in any direct fashion. The chief system administrator does review the log information available on a daily basis, checking for unusual activities on the part of the staff. Auditing of the use of the application programs maintained on the system has been the responsibility of the application program staff. The system administrator stated that since there is no charge-back for system usage tracking of the application users was deemed unnecessary.

RISK: This lack of detailed audit logs leaves the system incapable of tracking the use of the system. The system administrative staff has no audit trail to uncover what process may have caused a malfunction on the system and no true way, at the system level, of knowing who has accessed FTI data.

RECOMMENDATION: EDD management should require the UNIX administrators to establish audit trails to capture activities for all users of the system, including system administrators. The audit trail must be expanded to:

1. Capture all successful login and logoff attempts.
2. Capture all unsuccessful login and authorization attempts.
3. Capture all identification and authentication attempts.

4. Capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users).
5. Capture all actions, connections and requests performed by privileged functions.
6. Capture all changes to logical access control authorities (e.g., rights, permissions).
7. Capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
8. Capture the creation, modification and deletion of user accounts and group accounts.
9. Capture the creation, modification and deletion of user account and group account privileges.
10. Capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event.
11. Capture system startup and shutdown functions.
12. Capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s).
13. Capture the enabling or disabling of audit report generation services.
14. Capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.22 **FINDING**: According to the on-site evaluation performed the audit records are not maintained for a period required by IRS Publication 1075.

DISCUSSION: The UNIX system logs are rotated over a 30 day period. The system utilizes a cron job at week's end to move data to alternate storage and clear the system log storage area. Over the history of the AIX system this has been adequate storage of audit material.

RISK: While the current practice has been adequate it is possible that a longer retention period for system logs may be advisable. A flaw in the system might not cause an interruption in operations for several months. If that should be the case EDD has no ability to review the system logs. This will prevent an adequate correction of a fault in the system or system security.

RECOMMENDATION: EDD management should direct UNIX system administrators to maintain audit logs for a period of six (6) years. To conserve media, logs should be taken from the monthly log, already gathered, and consolidated on media removed from the system. This media should be stored in an alternate location, off-line. Policy should then fix a retention period for these audit logs. The IRS Publication 1075 specifies a retention period of six (6) years. See Section 5.6.2, Audit and Accountability, on page 22.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.23 **FINDING**: According to the on-site evaluation performed local or syslog server has enough space to capture and retain the logs generated by the system.

DISCUSSION: The procedure for capturing audit logs relies on a cron job to round robin the log for 30 days. The items in the logs are time stamped for use in log generation. Discussions with the system administrators revealed that log space has never been overrun.

RISK: The risk of having insufficient log space is that logs will either overwrite previous log entries or fail to record current activity. In either event vital data in the log audit record is lost making it impossible to reconstruct the causes of system failure or compromise. There will be insufficient data upon which to build corrective actions. It would then be possible for a perpetrator to have entered the system and seize or alter FTI data without an ability of system or investigative personnel to reconstruct the activity to asses the exposure, to identify the perpetrator, and to successfully have an untainted trail of evidence to use in prosecution of offenders.

RECOMMENDATION: None. All requirements have been met.

H.24 **FINDING**: According to the on-site evaluation performed EDD has no written procedure for audit review.

DISCUSSION: Having an informal, daily review of the system audit raises the possibility that either new personnel will be unaware of the procedure or current personnel will ignore what is only a local tradition without the support of a documented procedure. Although the interview revealed that only a select few individuals have authorized access to the UNIX system their activities need be audited and that audit trail reviewed.

RISK: The risk to FTI data and to the UNIX system is that an unauthorized user or disgruntled employee could commit malicious acts on the system compromising FTI data and such activity would be untraceable under the current audit conditions. Having no written policy requiring audit review renders no one responsible or liable for the audit review.

RECOMMENDATION: EDD management should develop a written policy requiring daily review of its UNIX system's audit.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the

Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Configuration Management – AIX

H.25 FINDING: According to the on-site evaluation performed the system does not use securetcpip.

DISCUSSION: Examination of the UNIX system and discussions with the UNIX system administrator disclosed that securetcpip is not installed and operational on the system.

RISK: Without securetcpip several communication protocols have settings that allow the running of untrusted commands and daemons. These commands may be activated by an application program or other user procedure and transmit FTI data to unauthorized procedures or users.

RECOMMENDATION: The EDD UNIX administrator should use the securetcpip command to provide enhanced security for the network. This command performs the following:

Runs the tcbck -a command, which disables the nontrusted commands and daemons: rcp, rlogin, rlogind, rsh, rshd, tftp, and tftpd. The disabled commands and daemons are not deleted; instead, they are changed to mode 0000. A particular command or daemon can be enabled by re-establishing a valid mode.

Adds a TCP/IP security stanza to the /etc/security/config file. The stanza is in the following format:

```
tcpip:
  netrc = ftp,rexec     /* functions disabling netrc */
```

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

System & Communications Protection – AIX

H.26 **FINDING**: According to the on-site evaluation performed the UNIX system does not terminate a network connection after 15 minutes of inactivity.

DISCUSSION: Examination of system configuration files and discussion with UNIX administrators disclosed that there is no session termination after a period of inactivity at the system level. The rationale put forth is that the facility is a closed facility and there are only a very limited number of individuals at the facility with authorized access to the UNIX system. It was therefore the opinion of the UNIX administrator that termination for inactivity was unwarranted.

RISK: The risk of having no termination after a period of 15 minutes of inactivity, is that the session can be pirated by another user who will then have unauthorized access to system resources including FTI data.

RECOMMENDATION: The EDD UNIX administrator should implement session termination for all sessions inactive for a period longer than 15 minutes.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

System Reviewed: DATA31 – Windows 2003 server

Identification & Authentication – Windows 2003

H.27 **FINDING**: According to the on-site evaluation performed password composition does not meet IRS Publication 1075 requirements.

DISCUSSION: Analysis of the Local Security Policy setting shows that:

1. Password length is not required to be between 8 and 128 characters, but fewer numbers of characters.
2. Passwords do not meet complexity requirement. The value for "Passwords Must Meet Complexity Requirements" is set to Disabled in the local security policy.

RISK: Without proper password length or complexity rules enforced, it is easier for an adversary to crack user passwords (especially for privileged accounts, such as System Administrators [SA] users), resulting in unauthorized system access and potential unauthorized disclosure of FTI data.

RECOMMENDATION: The following recommendations are suggested for the Windows server:

1. Open Local Security Policy
2. Ensure password length is set to 8 characters
3. Ensure password complexity setting is Enabled

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.28 **FINDING**: According to the on-site evaluation performed password aging settings do not meet IRS Publication 1075 requirements.

DISCUSSION: Analysis of the system Local Security Policy settings shows that the password aging requirement is not enforced. IRS Publication 1075 requires a minimum age of 15 days for all passwords. Windows password aging parameter is set to "0" days, which allows a user to change their password at any time, without waiting for the required 15 days. This means that, once a user changes their password, the user is not prevented from changing their password back to previous values.

A review of the system shows that there are only two administrators' accounts on the system and no user accounts. Therefore, the risk of this item is reduced, so long as normal user accounts are not added to the system.

RISK: Not enforcing password aging can allows a user to continue to use their old passwords, which may defeat the purpose of password aging.

RECOMMENDATION: The following recommendations are suggested for the Windows server:

1. Open the Local Security Policy.
2. Move to Password Policy.
3. Set the value for the "Minimum password age" to 15 days.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

Access Control – Windows 2003 Server

H.29 **FINDING**: According to the on-site evaluation performed vulnerable or unnecessary network services are enabled and running.

DISCUSSION: Analysis of the list of services on the server shows that vulnerable or unnecessary network services are enabled and running. For example, the following services are found to be running on the systems analyzed:

1. SNMP
2. Alerter
3. Remote Registry Service

Agency management indicated that SNMP is required for management of the system. The test revealed that Telnet, FTP, and Messenger are disabled.

RISK: Running unnecessary network services increases the risk of unauthorized access to the system and FTI. Enabling vulnerable or unnecessary services provides avenues for an attacker to compromise a system. The more services running on a computer, the more entry points you make available to unauthorized users. A service is a potential entry point because it processes client requests. To help reduce this risk, management should disable unnecessary system services.

SNMP service generates trap messages that are sent to a trap destination. A malicious user could utilize these services to perform a task that creates security vulnerability. Using insecure protocols such as SNMP provides eavesdropping capability for an adversary.

RECOMMENDATION: Institute a policy that mandates only required services necessary for the system to function are enabled. Further, implement SNMPv2 to replace SNMP.

Agency management should disable all running services that do not have a genuine business requirement for their existence on the Windows systems.

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.30 **FINDING**: According to the on-site evaluation performed the system allows anonymous enumeration of SAM accounts and shares.

DISCUSSION: Analysis of the Local Security Policy shows that the system permits anonymous access to SAM accounts and shares – anonymous network access to lookup account names, user groups, and file shares is not restricted. Providing NULL session connections allows an attacker or malicious user to access system resources without authentication.

RISK: Permitting anonymous access to SAM accounts and shares (NULL session connections) allows an attacker or malicious user to access confidential login credentials, list account names and enumerate share names. This information can later be used to launch other attacks. For example, a malicious individual could use this information to foot print a system. Foot printing is the process of gathering information about a system before an unauthorized user attempts to hack the computer and access FTI.

RECOMMENDATION: Using Microsoft Windows Local Security Policy tool:

Set the value for the Security Option, "Network access: Do not allow anonymous enumeration of SAM accounts and shares" to "Enabled"

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.31 **FINDING**: According to the on-site evaluation performed encryption is not being used when accessing Windows ("remote desktop") from other systems in the network.

DISCUSSION: A review of the registry setting shows that encryption is not being used when remotely accessing Windows operating system from other systems within or outside the network. There is no value set for the required registry key:

HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Conferencing\
Value Name: NoRDS

During the testing, EDD management indicated that encryption is not required for all communications within EDD's internal network.

RISK: Failure to use encryption to protect the confidentiality of remote access sessions can result in data interception by an unauthorized third-party eavesdropping on a network connection between EDD's system and an authorized user.

RECOMMENDATION: To ensure that encryption is being used when accessing Windows from other systems, create the registry key below and set the value to 1:

HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Conferencing\
Value Name: NoRDS

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.32 **FINDING**: According to the on-site evaluation performed Windows Messenger Internet Access is enabled.

DISCUSSION: A review of the registry setting shows that Windows Messenger Internet access is enabled. In addition, users can launch Windows Messenger (MSN Messenger, .NET Messenger). There is no Messenger sub key.

A review of the system shows that there are only two administrator accounts on the system and no user accounts. Therefore, the risk of this item is reduced, so long as normal user accounts are not added to the system.

RISK: Enabling Windows Messenger Internet Access could result in potential confidential FTI data or data files being transmitted to other systems.

RECOMMENDATION: Although normal user accounts are not present in the system currently, Windows messenger needs to be disabled in case users are created on the local system.

Create the registry keys below and set the value to 1:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Messenger\Client\{9b017612-c9f1-11d2-8d9f-0000f875c541}

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Messenger\Client
Value Name: PreventRun

AGENCY REPONSE: The EDD uses a shared environment for hosting several of the systems in question at the State of California's DTS, the statewide data center. The ability for the EDD to implement mitigation efforts for many of the current audit findings is limited by statewide priorities, resource availability, and funding by some or all of the customers of the statewide data center. Changes requested and made on behalf of the EDD will affect many departments within California. This will require in-depth analysis and planning activities to identify interdependencies, required funding and staffing, and available resources. The EDD will engage in this analysis and planning over the next 180 days to determine how to mitigate findings or the impact of accepting risks. The EDD will provide updates on specific implementation and mitigation efforts for each finding during regular update cycles.

IRS COMMENT: Agency response is accepted. Please report finding remediation status and planned/actual date in the next SAR as directed by the Office of Safeguards. Finding closure will be tracked through the IRS Office of Safeguards POA&M process.

H.33 **FINDING**: According to the on-site evaluation performed there are irrelevant files and registry entries in the system.

DISCUSSION: A review of the registry shows that there are no entries for the keys searched. Further, a listing of the "dllcache" directory does not show irrelevant files. In addition, there is no "os2" directory in the file system. However, the keys "Optional" and "Posix" exist.